ESET Smart Security 4

Benutzerhandbuch

(geeignet für Produktversion 4.2 und höher)

Microsoft® Windows® 7 / Vista / XP / 2000 / 2003 / 2008

ESET Smart Security 4

Copyright © 2010 ESET, spol. s r. o.

ESET Smart Security 4 wurde von ESET, spol. s r.o. entwickelt.
Weitere Informationen finden Sie unter www.eset.com.
Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Genehmigung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnehmen, Scannen oder auf andere Art.
ESET, spol. s r.o. behält sich das Recht vor, die beschriebene Anwendungssoftware ohne vorherige Ankündigung zu ändern.

Weltweiter Kundendienst: www.eset.eu/support
Kundendienst für Nordamerika: www.eset.com/support

REV.20100407-016

Inhalt

1. ESET Smart Security 4 4
1.1 Neuigkeiten 4
1.2 Systemanforderungen 5

2. Installation 6
2.1 Typische Installationsart 6
2.2 Benutzerdefinierte Installation 7
2.3 Vorhandene Einstellungen verwenden 9
2.4 Benutzernamen und Passwort eingeben 9
2.5 Manuelles Prüfen des Computers 9

3. Erste Schritte 10
3.1 Übersicht zur Benutzeroberfläche–Modi 10
3.1.1 Prüfen der Funktionsfähigkeit des Systems 10
3.1.2 Vorgehensweise bei fehlerhafter Ausführung des Programms 11
3.2 Einstellungen für Updates 11
3.3 Einstellungen der vertrauenswürdigen Zone 11
3.4 Einstellungen für den Proxyserver 12
3.5 Einstellungen schützen 12

4. Mit ESET Smart Security arbeiten 13
4.1 Viren- und Spyware-Schutz 13
4.1.1 Echtzeit-Dateischutz 13
4.1.1.1 Prüfeinstellungen 13
4.1.1.1.1 Zu prüfende Datenträger 13
4.1.1.1.2 Prüfen bei Ereignis 13
4.1.1.1.3 Zusätzliche ThreatSense-Einstellungen für neu erstellte und geänderte Dateien 13
4.1.1.1.4 Erweiterte Einstellungen 13
4.1.1.2 Entfernungsstufen 13
4.1.1.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden? 14
4.1.1.4 Echtzeit-Dateischutz prüfen 14
4.1.1.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz 14
4.1.2 Host Intrusion Prevention System (HIPS) 14
4.1.3 E-Mail-Client-Schutz 14
4.1.3.1 POP3-Prüfung 14
4.1.3.1.1 Kompatibilität 15
4.1.3.2 Integration in E-Mail-Programme 15
4.1.3.2.1 E-Mail-Nachrichtentexten Prüfhinweise hinzufügen 15
4.1.3.3 Eingedrungene Schadsoftware entfernen 16
4.1.4 Web-Schutz 16
4.1.4.1 HTTP, HTTPs 16
4.1.4.1.1 Adressverwaltung 16
4.1.4.1.2 Webbrowser 16
4.1.5 Computer prüfen 17
4.1.5.1 Prüfmethode 17
4.1.5.1.1 Standardprüfung 17
4.1.5.1.2 Prüfen mit speziellen Einstellungen 17
4.1.5.2 Zu prüfende Objekte 18
4.1.5.3 Prüfprofile 18
4.1.6 Prüfen von Anwendungsprotokollen 18

4.1.6.1 SSL ... 18
4.1.6.1.1 Vertrauenswürdige Zertifikate ... 19
4.1.6.1.2 Ausgeschlossene Zertifikate ... 19
4.1.7 Einstellungen für ThreatSense ... 19
4.1.7.1 Einstellungen für zu prüfende Objekte ... 19
4.1.7.2 Optionen ... 20
4.1.7.3 Schadcode entfernen ... 20
4.1.7.4 Dateierweiterungen ... 20
4.1.7.5 Grenzen ... 21
4.1.7.6 Sonstiges ... 21
4.1.8 Eingedrungene Schadsoftware wurde erkannt ... 21
4.2 Personal Firewall ... 22
4.2.1 Filtermodus ... 22
4.2.2 Profile ... 22
4.2.2.1 Profilverwaltung ... 22
4.2.3 Alle Netzwerkverbindungen blockieren: Vom Netzwerk trennen ... 23
4.2.4 Filter deaktivieren: Firewall deaktivieren ... 23
4.2.5 Regeln konfigurieren und verwenden ... 23
4.2.5.1 Neue Regel hinzufügen ... 23
4.2.5.2 Regeln bearbeiten ... 24
4.2.6 Zonen konfigurieren ... 24
4.2.6.1 Netzwerkauthentifizierung ... 24
4.2.6.1.1 Zonenauthentifizierung – Client-Konfiguration ... 24
4.2.6.1.2 Zonenauthentifizierung – Server-Konfiguration ... 25
4.2.7 Verbindung herstellen – Erkennung ... 26
4.2.8 Erstellen von Logs ... 26
4.3 Spam-Schutz ... 27
4.3.1 Intelligenter Spam-Schutz ... 27
4.3.1.1 Adressen zur Whitelist hinzufügen ... 27
4.3.1.2 E-Mails als Spam einstufen ... 27
4.4 Programm aktualisieren ... 28
4.4.1 Update-Einstellungen ... 28
4.4.1.1 Update-Profile ... 28
4.4.1.2 Erweiterte Einstellungen für Updates ... 28
4.4.1.2.1 Update-Modus ... 29
4.4.1.2.2 Proxyserver ... 29
4.4.1.2.3 LAN-Verbindungen ... 30
4.4.1.2.4 Erstellen von Update-Kopien–Update-Mirror ... 30
4.4.1.2.4.1 Aktualisieren über Update-Mirror ... 30
4.4.1.2.4.2 Fehlerbehebung bei Updates über Update-Mirror ... 31
4.4.2 So erstellen Sie Update-Tasks ... 32
4.5 Taskplaner ... 32
4.5.1 Verwendung von Tasks ... 32
4.5.2 Erstellen von Tasks ... 32
4.6 Quarantäne ... 33
4.6.1 Quarantäne für Dateien ... 33
4.6.2 Wiederherstellen aus der Quarantäne ... 33
4.6.3 Senden von Dateien in Quarantäne ... 33
4.7 Log-Dateien ... 33
4.7.1 Log-Wartung ... 34
4.8 Benutzeroberfläche ... 34
4.8.1 Warnungen und Hinweise ... 35
4.9 ThreatSense.Net ... 35
4.9.1 Verdächtige Dateien ... 36
4.9.2 Statistik ... 36
4.9.3 Senden ... 37
4.10 Remoteverwaltung ... 37
4.11 Lizenz ... 37

5. Erfahrene Benutzer ... 38

5.1 Einstellungen für den Proxyserver ... 38
5.2 Einstellungen exportieren/importieren ... 39
5.2.1 Einstellungen exportieren ... 39
5.2.2 Einstellungen importieren ... 39
5.3 Kommandozeile ... 39
5.4 ESET SysInspector ... 40
5.4.1 Verwendung von Benutzeroberfläche und Anwendung ... 40
5.4.1.1 Programmsteuerung ... 40
5.4.1.2 Navigation in ESET SysInspector ... 41
5.4.1.3 Vergleichen ... 41
5.4.1.4 SysInspector als Bestandteil von ESET Smart Security 4 ... 42
5.4.1.5 Dienste-Skript ... 42
5.5 ESET SysRescue ... 44
5.5.1 Minimalanforderungen ... 44
5.5.2 So erstellen Sie eine Rettungs-CD ... 44
5.5.2.1 Ordner ... 44
5.5.2.2 ESET Antivirus ... 44
5.5.2.3 Erweitert ... 45
5.5.2.4 Bootfähiges USB-Gerät ... 45
5.5.2.5 Brennen ... 45
5.5.3 Arbeiten mit ESET SysRescue ... 45
5.5.3.1 ESET SysRescue verwenden ... 45

6. Glossar ... 46

6.1 Schadsoftwaretypen ... 46
6.1.1 Viren ... 46
6.1.2 Würmer ... 46
6.1.3 Trojaner ... 46
6.1.4 Rootkits ... 46
6.1.5 Adware ... 47
6.1.6 Spyware ... 47
6.1.7 Potenziell unsichere Anwendungen ... 47
6.1.8 Eventuell unerwünschte Anwendungen ... 47
6.2 Remote-Angriffe ... 47
6.2.1 DoS-Angriffe ... 47
6.2.2 DNS Poisoning ... 47
6.2.3 Angriffe mit Würmern ... 48
6.2.4 Portscans (Port Scanning) ... 48
6.2.5 TCP Desynchronization ... 48
6.2.6 SMB Relay ... 48
6.2.7 ICMP-Angriffe ... 48
6.3 E-Mail ... 48
6.3.1 Werbung ... 49
6.3.2 Falschmeldungen (Hoaxes) ... 49
6.3.3 Phishing ... 49
6.3.4 Erkennen von Spam-Mails ... 49
6.3.4.1 Regeln ... 49
6.3.4.2 Bayesscher Filter ... 50
6.3.4.3 Whitelist ... 50
6.3.4.4 Blacklist ... 50
6.3.4.5 Serverseitige Kontrolle ... 50

1. ESET Smart Security 4

ESET Smart Security 4 ist der erste Vertreter eines neuen Ansatzes für wirklich integrierte Computersicherheit. Es nutzt die Geschwindigkeit und Präzision von ESET NOD32 Antivirus, die durch Verwendung der neuesten Version der ThreatSense® Prüf-Engine in Kombination mit der maßgeschneiderten Personal Firewall und dem Spam-Schutz gewährleistet sind. Auf diese Weise ist ein intelligentes System entstanden, das permanent vor Angriffen und bösartiger Software auf der Hut ist, die Ihren Computer gefährden.

Bei ESET Smart Security handelt es sich nicht um ein schwerfälliges Sammelsurium verschiedener zu einem Paket zusammengeschnürter Produkte, wie man es bei anderen Anbietern findet. Vielmehr ist es das Ergebnis langfristiger Bemühungen, maximalen Schutz bei minimaler Systembelastung zu bieten. Mithilfe der auf künstlicher Intelligenz basierenden Spitzentechnologien können das Eindringen von Viren, Spyware, Trojanern, Würmern, Adware, Rootkits und andere durch das Internet übertragene Angriffe aktiv verhindert werden, ohne dass die Systemleistung beeinträchtigt oder Ihr Computer vom Netz getrennt wird.

1.1 Neuigkeiten

Die langjährige Erfahrung unserer Fachleute im Entwicklungsbereich wird durch die vollkommen neuartige Architektur von ESET Smart Security unter Beweis gestellt, die bei minimalen Systemanforderungen einen maximalen Schutz gewährleistet. Diese zuverlässige Sicherheitslösung umfasst Module mit mehreren erweiterten Optionen. In der folgenden Liste erhalten Sie einen kurzen Überblick über diese Module.

- **Viren- und Spyware-Schutz**

Das Herzstück dieses Moduls bildet der Prüfmechanismus von ThreatSense®, der bei dem preisgekrönten NOD32 Antivirus-System erstmals zum Einsatz gekommen ist. ThreatSense® wurde für die neue Architektur von ESET Smart Security nochmals optimiert und verbessert.

Funktion	Beschreibung
Verbessertes Entfernen von Schadcode	Das Virenschutzsystem kann selbstständig einen Großteil der erkannten eingedrungenen Schadsoftware ohne ein Eingreifen des Benutzers entfernen und löschen.
Modus für Hintergrundprüfungen	Die Überprüfung des Computers kann im Hintergrund gestartet werden, ohne seine Leistung zu beeinträchtigen.
Kleinere Update-Dateien	Dank grundlegender Optimierungsprozesse sind die Update-Dateien kleiner als in Version 2.7. Auch der Schutz der Update-Dateien vor Beschädigungen wurde verbessert.
Schutz gängiger E-Mail-Programme	Ab sofort können eingehende E-Mails nicht nur in Microsoft Outlook, sondern auch in Outlook Express, Windows Mail, Windows Live Mail und Mozilla Thunderbird geprüft werden.
Weitere kleine Verbesserungen	– Der direkte Zugriff auf Dateisysteme sorgt für hohe Geschwindigkeit und einen schnellen Datendurchsatz. – Der Zugriff auf infizierte Dateien wird blockiert. – Optimierung für Windows-Sicherheitscenter, einschließlich Vista.

- **Personal Firewall**

Personal Firewall überwacht den gesamten Datenverkehr zwischen einem geschützten Computer und anderen Computern im Netzwerk. Im Folgenden sind die erweiterten Funktionen von ESET Personal Firewall aufgeführt.

Funktion	Beschreibung
Profile	Profile sind ein Hilfsmittel, um das Verhalten der Personal Firewall von ESET Smart Security zu steuern. Durch mehrere Profile, denen unterschiedliche Regeln zuweisbar sind, können Benutzer das Verhalten der Personal Firewall mühelos anpassen.
Zonenauthentifizierung	Anhand dieser Information können Benutzer das Netzwerk identifizieren, mit dem eine Verbindung hergestellt wird, und eine entsprechende Aktion definieren (z. B. Wechsel des Firewall-Profils oder Blockieren der Kommunikation in diese Zone).
Prüfung der Netzwerkverbindungen auf niedriger Schicht	Durch Prüfung der Netzwerkverbindungen auf der Verbindungssicherungsschicht ist ESET Personal Firewall in der Lage, eine Vielzahl von Angriffen abzuwehren, die andernfalls nicht erkannt würden.
IPv6-Unterstützung	ESET Personal Firewall zeigt IPv6-Adressen an und bietet Benutzern die Möglichkeit, Regeln für sie festzulegen.
Überwachung ausführbarer Dateien	Änderungen innerhalb ausführbarer Dateien werden zur Abwehr möglicher Infektionen überwacht. Dateiänderungen durch signierte Anwendungen können zugelassen werden.
Prüfung von Dateien innerhalb der Protokolle HTTP(s) und POP3(s)	Dateien werden auch innerhalb der Anwendungsprotokolle HTTP(s) und POP3(s) geprüft. Benutzer sind daher auch beim Surfen im Internet und Herunterladen von E-Mails geschützt.
System zur Erkennung von Eindringungsversuchen	Die Art der Netzwerkverbindung sowie verschiedene Formen von Netzwerkangriffen werden erkannt; zusätzlich gibt es die Option, diese Verbindungen automatisch zu verhindern.
Interaktiver Filtermodus, regelbasierter Filtermodus, Trainingsmodus und automatischer Filtermodus mit Ausnahmen	Benutzer können wählen, ob die Firewall-Aktionen automatisch ausgeführt werden sollen, oder ob sie dafür interaktiv Regeln erstellen wollen. Im regelbasierten Filtermodus werden Verbindungen anhand von Regeln geprüft, die zuvor durch den Benutzer oder den Netzwerkadministrator festgelegt wurden. Im Trainingsmodus werden Regeln automatisch erstellt und gespeichert. Dieser Modus ist für die anfängliche Konfiguration der Firewall geeignet.
Ersetzt die integrierte Windows-Firewall	Ersetzt die integrierte Windows Firewall und interagiert mit dem Windows Security Center, um den Sicherheitsstatus zu überwachen. Bei der Installation von ESET Smart Security wird die Windows-Firewall standardmäßig deaktiviert.

- **Antispam (Spam-Schutz)**

ESET Antispam prüft unerwünschte E-Mails und erhöht somit die Sicherheit und den Komfort der elektronischen Kommunikation.

Funktion	Beschreibung
Einstufung eingehender E-Mails	Jede eingehende E-Mail wird mithilfe einer Bewertungsskala von 0 (die Nachricht ist nicht als Spam zu bewerten) bis 100 (die Nachricht ist als Spam zu bewerten) eingestuft. Je nach Einstufung wird die E-Mail dann in den Ordner für Spam oder in einen vom Nutzer angelegten und definierten Ordner weitergeleitet. Die parallele Prüfung eingehender E-Mails ist möglich.
Unterstützung einer Vielzahl von Prüftechniken	– Bayesscher Filter – Regelbasierte Prüfung – Abgleich mit einer globalen Fingerprint-Datenbank
Vollständige Integration in E-Mail-Programme	Der Spam-Schutz steht Benutzern von Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail und Mozilla Thunderbird zur Verfügung.
Manuelle Markierung als Spam	E-Mails können optional auch manuell als Spam / kein Spam markiert werden.

- **Weitere Funktionen**

Funktion	Beschreibung
ESET SysRescue	Mit ESET SysRescue können Benutzer ein bootfähiges Medium (CD/DVD/USB) mit ESET Smart Security erstellen, das betriebssystemunabhängig ausführbar ist. Dies ist der beste Weg, um das System von schwer zu entfernender Schadsoftware zu befreien.
ESET SysInspector	ESET SysInspector ist eine Anwendung, die Ihren Computer gründlich untersucht. Sie ist nun fester Bestandteil von ESET Smart Security. Wenn Sie sich mittels der Option „Hilfe und Support" > „Supportanfrage" an den Supportservice wenden, können Sie einen mit ESET SysInspector erstellten Status-Snapshot Ihres Computers anfügen.
Dokumentschutz	Der Dokumentenschutz überprüft Microsoft Office-Dokumente vor dem Öffnen und automatisch von Internet Explorer heruntergeladene Dateien wie Microsoft ActiveX-Elemente.
Self Defense	Die neue Self Defense-Technologie schützt die Komponenten von ESET Smart Security vor Deaktivierungsversuchen.
Benutzeroberfläche	Die Benutzeroberfläche kann nun auch im nichtgrafischen Modus ausgeführt werden. Dadurch ist die Verwaltung von ESET Smart Security auch über die Tastatur möglich. Dank der erhöhten Kompatibilität mit Bildschirmleseprogrammen können auch sehbehinderte Personen das Programm effektiver verwalten.

1.2 Systemanforderungen

Für einen reibungslosen Betrieb von ESET Smart Security und ESET Smart Security Business Edition sollte Ihr System die folgenden Hardware- und Softwareanforderungen erfüllen:

ESET Smart Security:

Windows 2000, XP	400 MHz 32-Bit/64-Bit (x86/x64) 128 MB RAM-Arbeitsspeicher 35 MB freier Festplattenspeicher Super VGA (800 × 600)
Windows 7, Vista	1 GHz 32-Bit/64-Bit (x86/x64) 512 MB RAM-Arbeitsspeicher 35 MB freier Festplattenspeicher Super VGA (800 × 600)

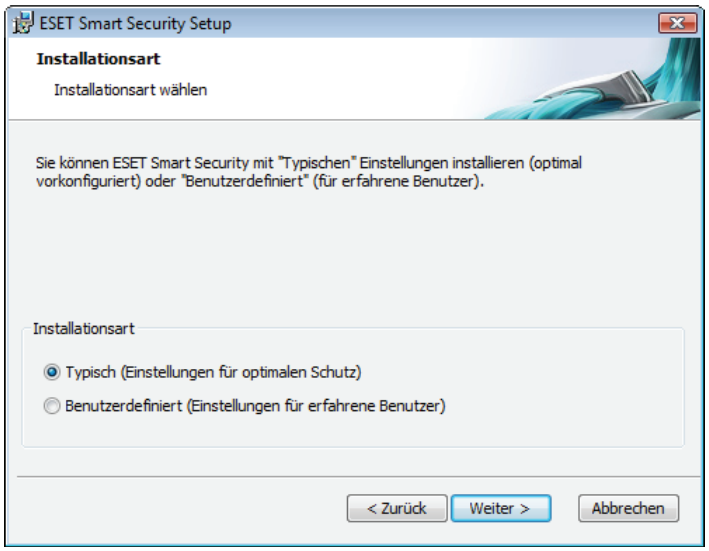
ESET Smart Security Business Edition:

Windows 2000, 2000 Server, XP, 2003 Server	400 MHz 32-Bit/64-Bit (x86/x64) 128 MB RAM-Arbeitsspeicher 35 MB freier Festplattenspeicher Super VGA (800 × 600)
Windows 7, Vista, Windows Server 2008	1 GHz 32-Bit/64-Bit (x86/x64) 512 MB RAM-Arbeitsspeicher 35 MB freier Festplattenspeicher Super VGA (800 × 600)

2. Installation

Nach dem Kauf des Programms können Sie das ESET Smart Security-Installationsprogramm von der ESET-Website herunterladen. Das entsprechende Paket heißt „ess_nt**_***.msi“ (ESET Smart Security) bzw. „essbe_nt**_***.msi“ (ESET Smart Security Business Edition). Starten Sie das Installationsprogramm. Der Installationsassistent unterstützt Sie bei der Installation. Es stehen zwei Installationsmodi zur Verfügung, die unterschiedlich viele Einstellungsmöglichkeiten bieten:

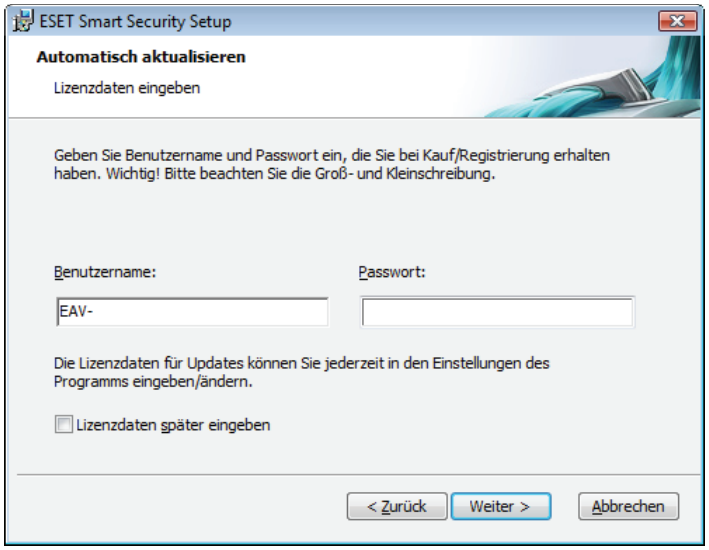
1. Standardinstallation
2. Benutzerdefinierte Installation


ESET Smart Security Setup
Installationsart
Installationsart wählen
Sie können ESET Smart Security mit "Typischen" Einstellungen installieren (optimal vorkonfiguriert) oder "Benutzerdefiniert" (für erfahrene Benutzer).
Installationsart
Typisch (Einstellungen für optimalen Schutz)
Benutzerdefiniert (Einstellungen für erfahrene Benutzer)
< Zurück
Weiter >
Abbrechen

2.1 Typische Installationsart

Die typische Installationsart wird Benutzern empfohlen, die ESET Smart Security mit den Standardeinstellungen installieren möchten. Die Standardeinstellungen des Programms bieten maximalen Schutz. Für weniger erfahrene Benutzer, die detaillierte Einstellungen nicht selbst vornehmen möchten, ist daher die typische Installationsart die richtige Wahl.

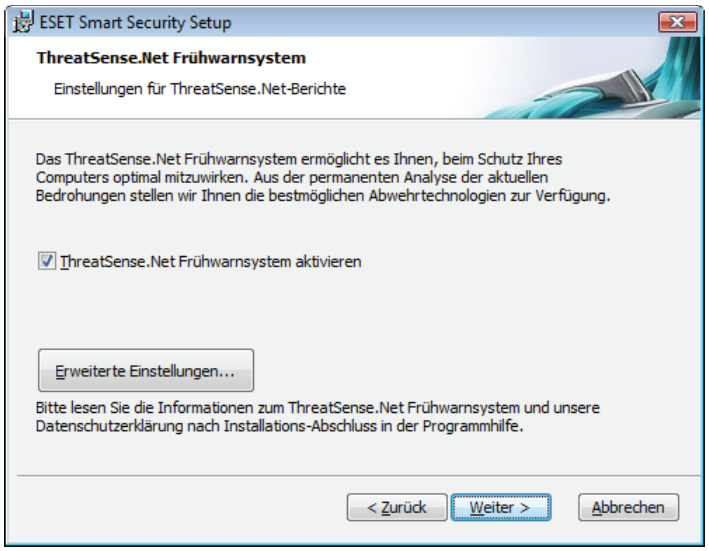
Der erste (sehr wichtige) Schritt ist die Eingabe des Benutzernamens und des Passworts für die automatische Aktualisierung des Programms. Dies ist erforderlich, damit ein kontinuierlicher Schutz des Systems gewährleistet werden kann.


ESET Smart Security Setup
Automatisch aktualisieren
Lizenzdaten eingeben
Geben Sie Benutzername und Passwort ein, die Sie bei Kauf/Registrierung erhalten haben. Wichtig! Bitte beachten Sie die Groß- und Kleinschreibung.
Benutzername:
Passwort:
EAV-
Die Lizenzdaten für Updates können Sie jederzeit in den Einstellungen des Programms eingeben/ändern.
Lizenzdaten später eingeben
< Zurück
Weiter >
Abbrechen

Geben Sie in den entsprechenden Feldern Ihren **Benutzernamen** und Ihr **Passwort** ein, also die Authentifizierungsdaten, die Sie beim Kauf oder bei der Registrierung des Produkts erhalten haben. Falls Sie Ihren Benutzernamen und Ihr Passwort gerade nicht zur Hand haben, wählen Sie die Option **Zugangsdaten später eingeben**.

Die Zugangsdaten können zu einem beliebigen späteren Zeitpunkt direkt vom Programm aus eingegeben werden.

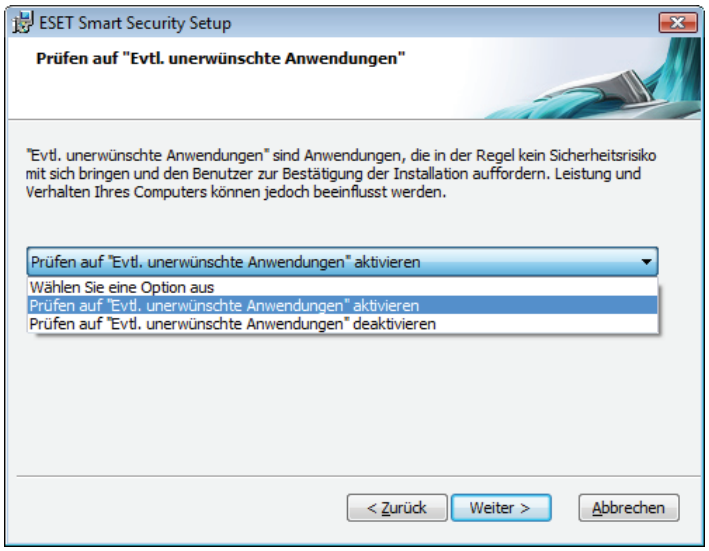
Der nächste Installationsschritt besteht in der Konfiguration des ThreatSense.Net-Frühwarnsystems. Über das ThreatSense.Net-Frühwarnsystem erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuer Schadsoftware, um dem Benutzer umfassenden Schutz zu bieten. Das Frühwarnsystem übermittelt neue Bedrohungen an ESET, wo die fraglichen Dateien analysiert, bearbeitet und zur Signaturdatenbank hinzugefügt werden.


ESET Smart Security Setup
ThreatSense.Net Frühwarnsystem
Einstellungen für ThreatSense.Net-Berichte
Das ThreatSense.Net Frühwarnsystem ermöglicht es Ihnen, beim Schutz Ihres Computers optimal mitzuwirken. Aus der permanenten Analyse der aktuellen Bedrohungen stellen wir Ihnen die bestmöglichen Abwehrtechnologien zur Verfügung.
ThreatSense.Net Frühwarnsystem aktivieren
Erweiterte Einstellungen...
Bitte lesen Sie die Informationen zum ThreatSense.Net Frühwarnsystem und unsere Datenschutzerklärung nach Installations-Abschluss in der Programmhilfe.
< Zurück
Weiter >
Abbrechen

Standardmäßig ist das Kontrollkästchen **ThreatSense.Net-Frühwarnsystem aktivieren** zum Aktivieren dieser Funktion aktiviert. Klicken Sie auf **Erweiterte Einstellungen**, um Einstellungen für das Einsenden verdächtiger Dateien festzulegen.

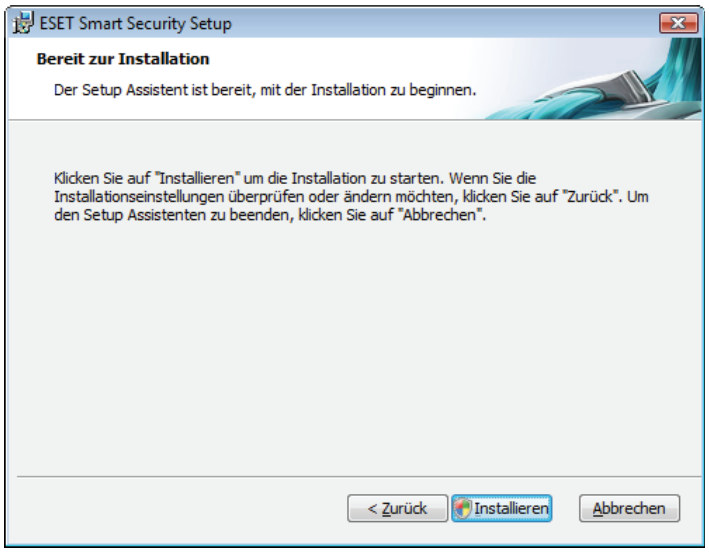
Der nächste Schritt im Installationsprozess ist die Konfiguration der Option **Prüfen auf evtl. unerwünschte Anwendungen**. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können.

Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.


ESET Smart Security Setup
Prüfen auf "Evtl. unerwünschte Anwendungen"
"Evtl. unerwünschte Anwendungen" sind Anwendungen, die in der Regel kein Sicherheitsrisiko mit sich bringen und den Benutzer zur Bestätigung der Installation auffordern. Leistung und Verhalten Ihres Computers können jedoch beeinflusst werden.
Prüfen auf "Evtl. unerwünschte Anwendungen" aktivieren
Wählen Sie eine Option aus
Prüfen auf "Evtl. unerwünschte Anwendungen" aktivieren
Prüfen auf "Evtl. unerwünschte Anwendungen" deaktivieren
< Zurück
Weiter >
Abbrechen

Aktivieren Sie die Option **Prüfen auf evtl. unerwünschte Anwendungen aktivieren**, um die Prüfung dieser Art von Bedrohung durch ESET Smart Security zuzulassen (empfohlen).

Der letzte Schritt im Standard-Installationsmodus ist die Bestätigung der Installation. Klicken Sie dazu auf die Schaltfläche **Installieren**.


ESET Smart Security Setup
Bereit zur Installation
Der Setup Assistent ist bereit, mit der Installation zu beginnen.
Klicken Sie auf "Installieren" um die Installation zu starten. Wenn Sie die Installationseinstellungen überprüfen oder ändern möchten, klicken Sie auf "Zurück". Um den Setup Assistenten zu beenden, klicken Sie auf "Abbrechen".
< Zurück
Installieren
Abbrechen

2.2 Benutzerdefinierte Installation

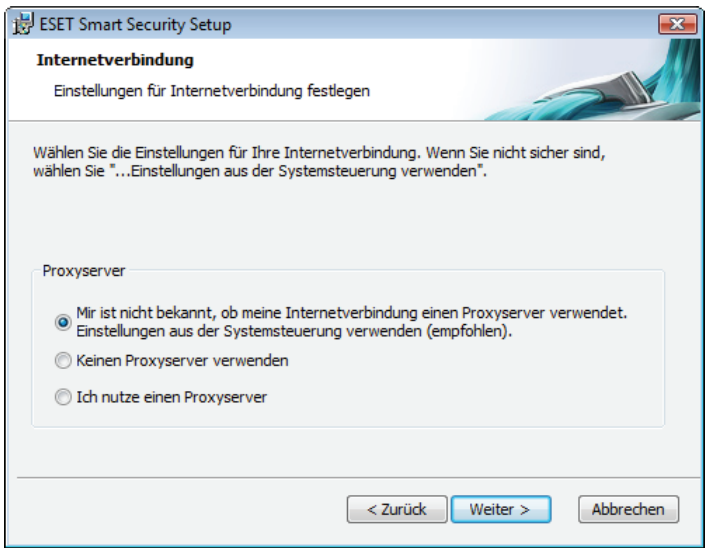
Die **benutzerdefinierte** Installation ist für erfahrene Benutzer geeignet, die während der Installation spezielle Einstellungen vornehmen möchten.

Zunächst wird das Zielverzeichnis für die Installation ausgewählt. Standardmäßig wird das Programm im Ordner C:\Programme\ESET\ESET Smart Security\ installiert. Klicken Sie auf **Durchsuchen...**, um einen anderen Speicherort anzugeben (nicht empfohlen).

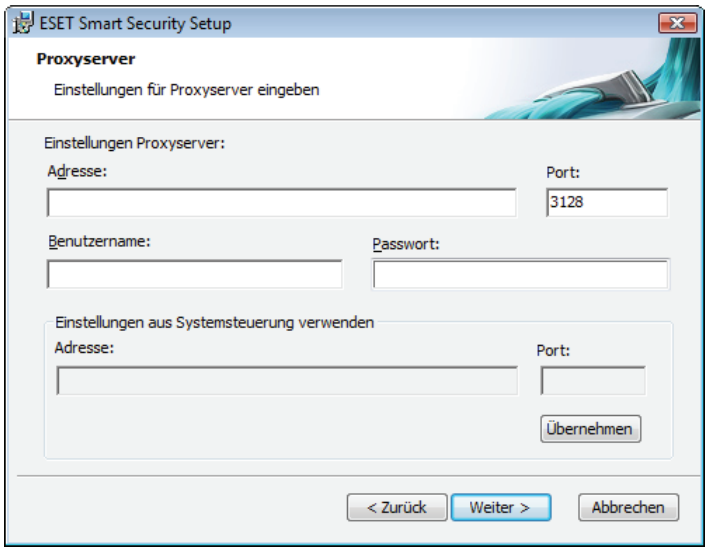
ESET Smart Security Setup
Installationsverzeichnis wählen
Installationsverzeichnis von ESET Smart Security.
Um in das angegebene Verzeichnis zu installieren, klicken Sie bitte "Weiter". Für ein alternatives Installationsverzeichnis klicken Sie bitte auf "Wählen".
Verzeichnis:
C:\Program Files\ESET\ESET Smart Security\
Wählen...
< Zurück
Weiter >
Abbrechen

Im nächsten Schritt müssen Sie **Benutzernamen und Passwort eingeben**. Dieser Schritt wird wie bei der Standardinstallation (siehe Seite 5) durchgeführt.

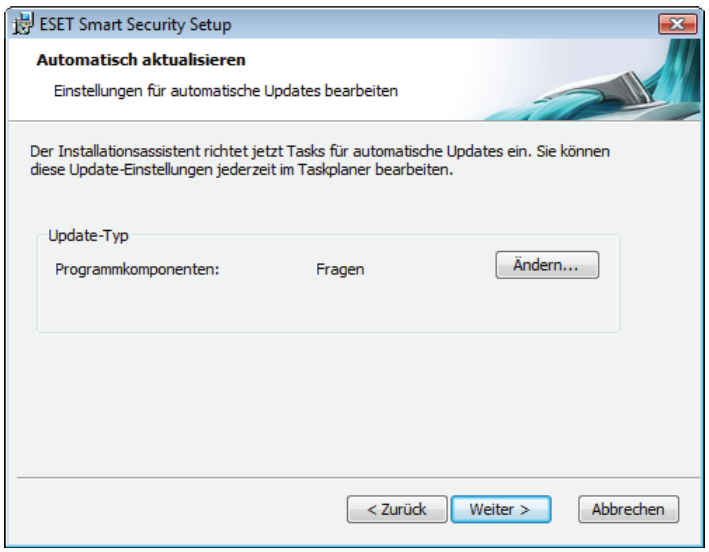
Nachdem Sie Benutzernamen und Passwort eingegeben haben, klicken Sie auf **Weiter**, um **Einstellungen für die Internetverbindung festzulegen**.


ESET Smart Security Setup
Internetverbindung
Einstellungen für Internetverbindung festlegen
Wählen Sie die Einstellungen für Ihre Internetverbindung. Wenn Sie nicht sicher sind, wählen Sie "...Einstellungen aus der Systemsteuerung verwenden".
Proxyserver
Mir ist nicht bekannt, ob meine Internetverbindung einen Proxyserver verwendet. Einstellungen aus der Systemsteuerung verwenden (empfohlen).
Keinen Proxyserver verwenden
Ich nutze einen Proxyserver
< Zurück
Weiter >
Abbrechen

Wenn Sie einen Proxyserver verwenden, muss dieser richtig konfiguriert sein, damit die Virensignaturen ordnungsgemäß aktualisiert werden können. Falls Sie nicht wissen, ob Sie einen Proxyserver für Internetverbindungen verwenden, wählen Sie die Standardeinstellung **Mir ist nicht bekannt, ob meine Internetverbindung einen Proxyserver verwendet. Internet Explorer-Einstellungen verwenden**, und klicken Sie auf **Weiter**. Falls Sie keinen Proxyserver verwenden, aktivieren Sie die entsprechende Option.

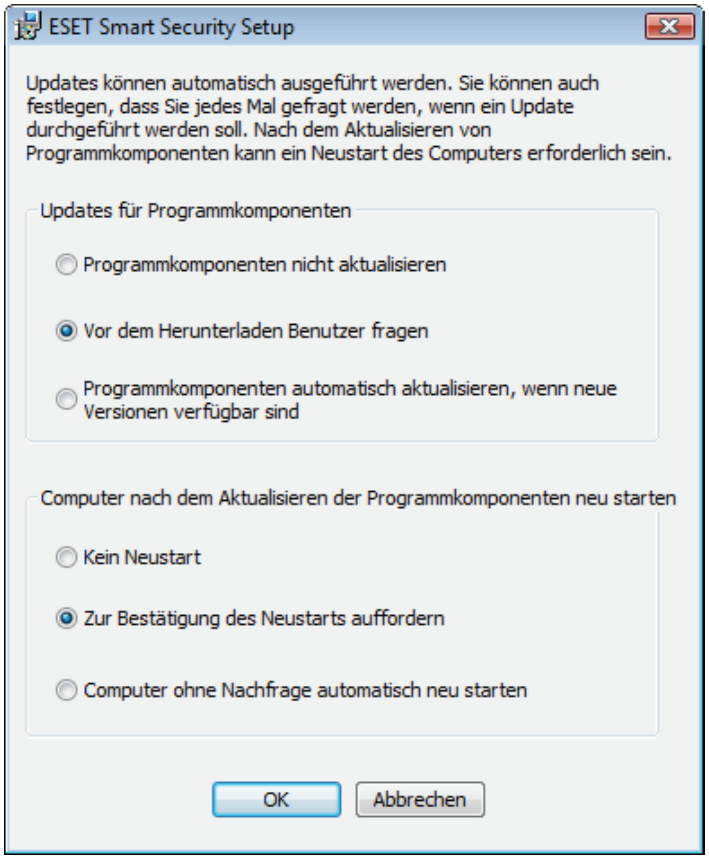


Um die Einstellungen für den Proxyserver vorzunehmen, wählen Sie **Ich nutze einen Proxyserver**, und klicken Sie auf **Weiter**. Geben Sie unter **Adresse** die IP-Adresse oder URL des Proxyservers ein. Unter **Port** können Sie den Port angeben, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver Zugangsdaten zur Authentifizierung erforderlich sind, geben Sie den gültigen Benutzernamen und das Passwort ein. Die Einstellungen für den Proxyserver können auch aus dem Internet Explorer kopiert werden, falls gewünscht. Klicken Sie dazu auf **Übernehmen**, und bestätigen Sie die Auswahl.



Klicken Sie auf **Weiter**, um mit dem Fenster **Einstellungen für automatische Updates bearbeiten** fortzufahren. In diesem Schritt können Sie festlegen, wie automatische Aktualisierungen von Programmkomponenten auf Ihrem System gehandhabt werden. Klicken Sie auf **Ändern...**, um erweiterte Einstellungen vorzunehmen.

Wenn Sie nicht möchten, dass Programmkomponenten aktualisiert werden, wählen Sie **Programmkomponenten nicht aktualisieren**. Wenn Sie die Option **Benutzer fragen** auswählen, wird ein Bestätigungsfenster für das Herunterladen von Programmkomponenten angezeigt. Um Programmkomponenten automatisch aktualisieren zu lassen, wählen Sie **Programmkomponenten automatisch aktualisieren, wenn neue Versionen verfügbar sind**.


ESET Smart Security Setup
Updates können automatisch ausgeführt werden. Sie können auch festlegen, dass Sie jedes Mal gefragt werden, wenn ein Update durchgeführt werden soll. Nach dem Aktualisieren von Programmkomponenten kann ein Neustart des Computers erforderlich sein.
Updates für Programmkomponenten
Programmkomponenten nicht aktualisieren
Vor dem Herunterladen Benutzer fragen
Programmkomponenten automatisch aktualisieren, wenn neue Versionen verfügbar sind
Computer nach dem Aktualisieren der Programmkomponenten neu starten
Kein Neustart
Zur Bestätigung des Neustarts auffordern
Computer ohne Nachfrage automatisch neu starten
OK
Abbrechen

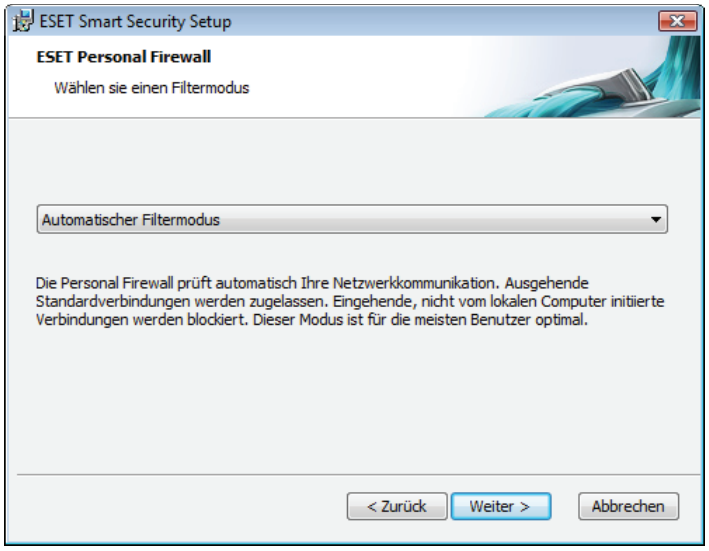
HINWEIS: Nach der Aktualisierung von Programmkomponenten muss der Computer üblicherweise neu gestartet werden. Dabei wird folgende Einstellung empfohlen: **Computer automatisch neu starten, ohne Nachfrage**.

Der nächste Schritt im Installationsprozess ist die Eingabe eines Passworts zum Schutz der Programmparameter. Wählen Sie ein Passwort zum Schutz des Programms. Geben Sie das Passwort zur Bestätigung erneut ein.

Die Schritte **Konfiguration des ThreatSense.Net-Frühwarnsystems** und **Prüfen auf evtl. unerwünschte Anwendungen** werden wie bei der Standardinstallation ausgeführt (siehe Seite 5).

Der letzte Schritt bei der benutzerdefinierten Installation ist die Auswahl des Filtermodus der ESET Personal Firewall. Es stehen fünf Modi zur Auswahl:

- Automatischer Filtermodus
- Automatischer Filtermodus mit Ausnahmen (benutzerdefinierte Regeln)
- Interaktiver Filtermodus
- Regelbasierter Filtermodus
- Trainingsmodus


ESET Smart Security Setup
ESET Personal Firewall
Wählen sie einen Filtermodus
Automatischer Filtermodus
Die Personal Firewall prüft automatisch Ihre Netzwerkkommunikation. Ausgehende Standardverbindungen werden zugelassen. Eingehende, nicht vom lokalen Computer initiierte Verbindungen werden blockiert. Dieser Modus ist für die meisten Benutzer optimal.
< Zurück
Weiter >
Abbrechen

Automatische Filtermodus empfohlen. Alle standardmäßigen ausgehenden Verbindungen werden aktiviert (die Analyse erfolgt anhand der vordefinierten Einstellungen automatisch), und unerwünschte eingehende Verbindungen werden automatisch blockiert.

Automatischer Filtermodus mit Ausnahmen (benutzerdefinierte Regeln). Zusätzlich zum automatischen Filtermodus ermöglicht es Ihnen der Modus, benutzerdefinierte Regeln hinzuzufügen.

interaktive Modus eignet sich für erfahrene Benutzer. Verbindungen werden auf der Basis benutzerdefinierter Regeln gesteuert. Falls für eine Verbindung keine Regel definiert ist, wird der Benutzer durch das Programm aufgefordert, die Verbindung zuzulassen oder zu blockieren.

Policy-Filtermodus werden Verbindungen anhand vordefinierter Regeln geprüft, die durch den Administrator festgelegt wurden. Falls keine Regel verfügbar ist, wird die Verbindung automatisch blockiert, ohne dass ein Hinweis angezeigt wird. Es wird empfohlen, den Policy-Filtermodus nur auszuwählen, wenn Sie die Netzwerkverbindungen als Administrator steuern möchten.

Trainingsmodul–Erstellt und speichert automatisch Regeln und ist geeignet für die anfängliche Konfiguration der Personal Firewall. Es ist kein Benutzereingriff erforderlich, da ESET Smart Security Regeln entsprechend vordefinierten Parametern speichert. Das Trainingsmodul ist nicht sicher und sollte nur verwendet werden, bis alle Regeln für die erforderlichen Kommunikationen erstellt wurden.

Im Anschluss wird ein Fenster angezeigt, in dem Sie die Installation bestätigen müssen.

2.3 Vorhandene Einstellungen verwenden

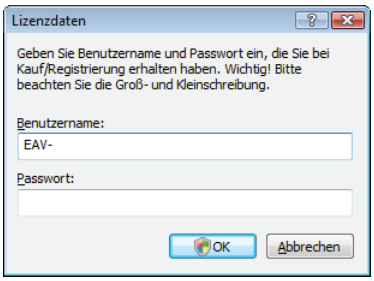
Wenn Sie ESET Smart Security neu installieren, wird die Option **Vorhandene Einstellungen übernehmen** angezeigt. Wählen Sie diese Option, um die Einstellungen der ersten Installation für die neue zu übernehmen.

ESET Smart Security Setup
Installationsart
Installationsart wählen
Wenn Sie die Option "Vorhandene Einstellungen übernehmen" aktivieren, werden diese bei der Neuinstallation beibehalten.
Deaktivieren Sie das Kontrollkästchen, wenn Sie die Einstellungen ändern möchten. Wählen Sie anschließend einen Installationsmodus.
Vorhandene Einstellungen übernehmen
Installationsart
Typisch (Einstellungen für optimalen Schutz)
Benutzerdefiniert (Einstellungen für erfahrene Benutzer)
< Zurück
Weiter >
Abbrechen

2.4 Benutzernamen und Passwort eingeben

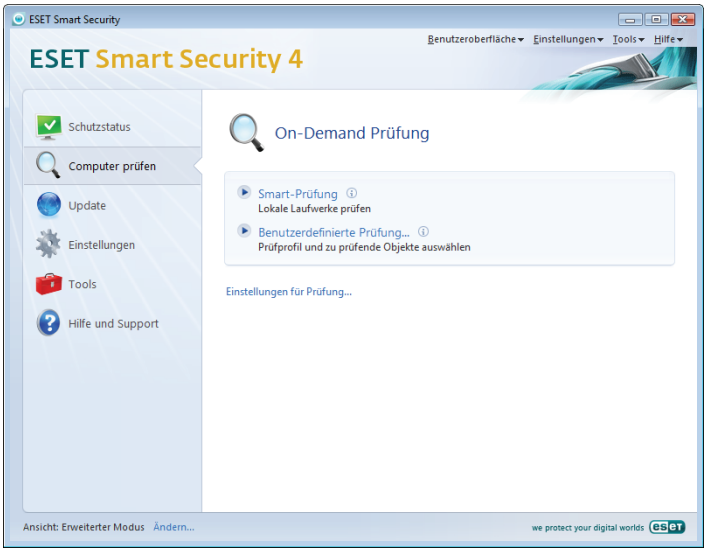
Damit alle Funktionen optimal genutzt werden können, sollte das Programm automatisch aktualisiert werden. Dies ist nur möglich, wenn Benutzername und Passwort in den Einstellungen für Updates eingegeben wurden.

Falls Sie Ihren Benutzernamen und das Passwort während des Installationsvorgangs nicht eingegeben haben, können Sie diese Daten wie folgt eintragen: Klicken Sie im Hauptprogrammfenster auf **Update** und dann auf **Benutzernamen und Passwort festlegen...**. Geben Sie die Daten, die Sie mit Ihrer Produktlizenz erhalten haben, im Fenster **Lizenzdaten** ein.



2.5 Manuelles Prüfen des Computers

Nach der Installation von ESET Smart Security sollte geprüft werden, ob auf dem Computer schädlicher Code vorhanden ist. Um eine schnelle Überprüfung auszuführen, wählen Sie im Hauptmenü **Computer prüfen**. Klicken Sie anschließend im Hauptprogrammfenster auf **Standardprüfung**. Weitere Informationen zu dieser Funktion finden Sie im Kapitel „Prüfen des Computers".



3. Erste Schritte

Dieses Kapitel liefert eine erste Übersicht über ESET Smart Security und die Grundeinstellungen des Programms.

3.1 Übersicht zur Benutzeroberfläche–Modi

Das Hauptfenster von ESET Smart Security ist in zwei Abschnitte unterteilt. In der schmaleren Spalte auf der linken Seite können Sie auf das benutzerfreundliche Hauptmenü zugreifen. Das Hauptprogrammfenster auf der rechten Seite dient vor allem zur Anzeige von Informationen zu der im Hauptmenü ausgewählten Option.

Im Folgenden werden die Schaltflächen des Hauptmenüs beschrieben.

Schutzstatus – In benutzerfreundlicherForm werden Informationen zum Schutzstatus von ESET Smart Security angezeigt. Wenn der erweiterte Modus aktiviert ist, wird der Status aller Schutzmodule angezeigt. Klicken Sie auf ein Modul, um dessen aktuellen Status anzuzeigen.

Prüfen des Computers – In diesem Abschnitt kann bei Bedarf eine Prüfung des Computers gestartet werden.

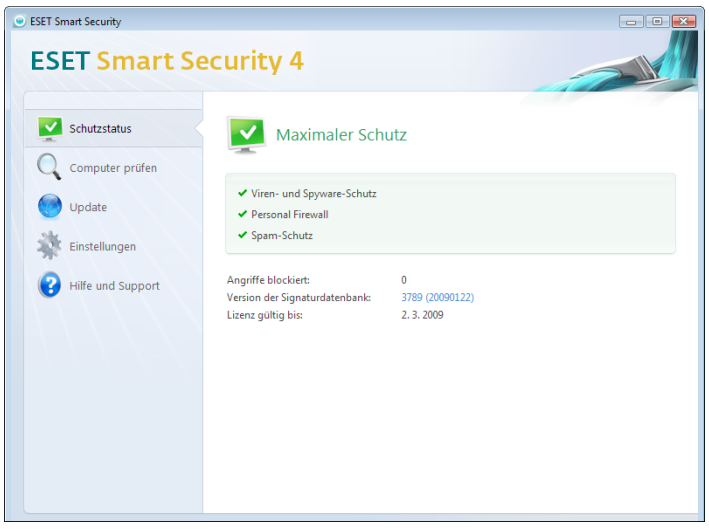
Update – Wählen Sie diese Option, um das Update-Modul aufzurufen, mit dem Updates für Programme verwaltet werden können.

Einstellungen – Wählen Sie diese Option, um die Sicherheitsstufe Ihres Computers anzupassen. Im erweiterten Modus werden zusätzlich die Untermenüs für Viren- und Spyware-Schutz, Personal Firewall und Spam-Schutz-Modul angezeigt.

Extras – Diese Option steht nur im erweiterten Modus zur Verfügung. Sie erlaubt den Zugriff auf Log-Dateien, Quarantäne und den Taskplaner.

Hilfe und Support – Wählen Sie diese Option, um auf die Datenbank und die Website von ESET zuzugreifen oder den Kundendienst anzufordern.

Innerhalb der Benutzeroberfläche von ESET Smart Security kann der Benutzer zwischen dem Standardmodus und dem erweiterten Modus wechseln. Um zwischen diesen Einstellungen umzuschalten, nutzen Sie den Link **Anzeige** unten links im Hauptbildschirm von ESET Smart Security. Klicken Sie auf diese Schaltfläche, um den gewünschten Anzeigemodus auszuwählen.



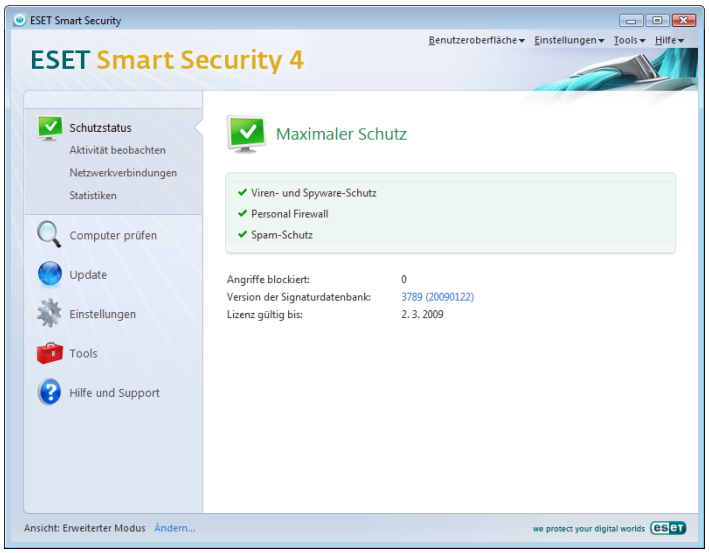
Im Standardmodus können Sie auf Funktionen zugreifen, die für allgemeine Vorgänge benötigt werden. Die erweiterten Einstellungen werden nicht angezeigt.

Beim Wechsel in den erweiterten Modus wird dem Hauptmenü die Option **Extras** hinzugefügt. Über die Option „Extras" können Sie auf Taskplaner und Quarantäne zugreifen und Log-Dateien von ESET Smart Security anzeigen.

HINWEIS: Die weiteren Anweisungen in diesem Handbuch beziehen sich auf den erweiterten Modus.

3.1.1 Prüfen der Funktionsfähigkeit des Systems

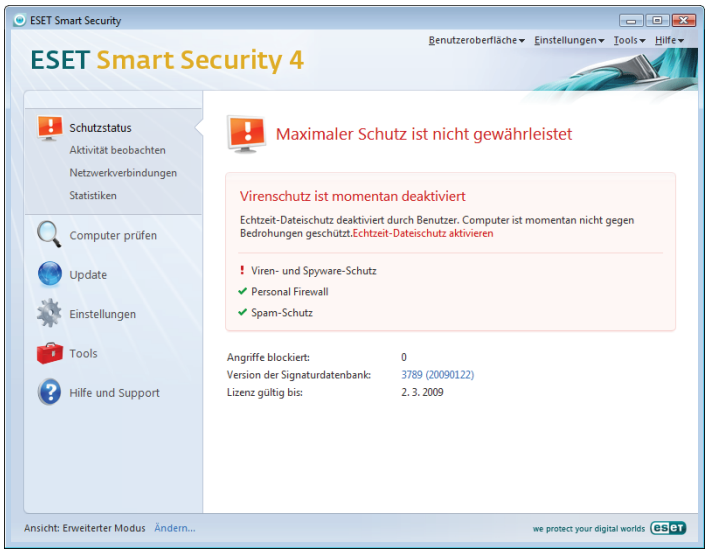
Zum Anzeigen des **Schutzstatus** klicken Sie oben im Hauptmenü auf die entsprechende Option. Auf der rechten Seite des Fensters befindet sich eine Darstellung des aktuellen Betriebszustands von ESET Smart Security, außerdem wird ein Untermenü mit drei Optionen angezeigt: **Viren- und Spyware-Schutz**, **Personal Firewall** und **Spam-Schutz-Modul**. Wenn Sie eine dieser Optionen auswählen, werden ausführlichere Informationen zu dem entsprechenden Modul angezeigt.



Wenn die aktivierten Module ordnungsgemäß arbeiten, sind sie grün markiert. Andernfalls wird ein rotes oder orangefarbenes Symbol angezeigt. Weitere Informationen zu dem Modul erhalten Sie im oberen Teil des Fensters. Unter anderem finden Sie dort einen Vorschlag zur Behebung des Problems. Um den Status einzelner Module zu ändern, klicken Sie im Hauptmenü auf **Einstellungen**, und wählen Sie das gewünschte Modul aus.

3.1.2 Vorgehensweise bei fehlerhafter Ausführung des Programms

Wenn ESET Smart Security ein Problem bei einem der Schutzmodule entdeckt, wird dies im Fenster **Schutzstatus** gemeldet. Hier finden Sie auch eine mögliche Lösung für das Problem.

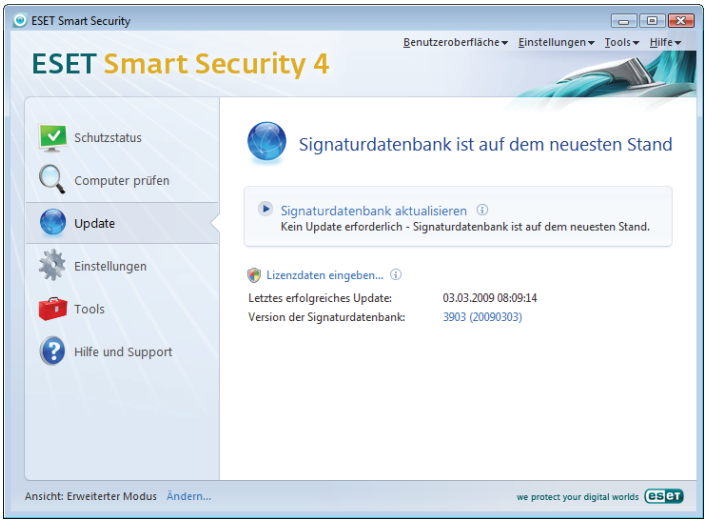


Wenn sich ein Problem nicht anhand der Liste bekannter Probleme und Lösungen beheben lässt, klicken Sie auf **Hilfe und Support**, um die Hilfedateien aufzurufen oder in der Datenbank zu suchen. Wenn Sie auch hier keine Lösung finden, können Sie eine Kundendienstanfrage an den ESET-Kundendienst senden. Auf Grundlage dieser Rückmeldungen können unsere Spezialisten Ihre Fragen schnell beantworten und Sie effektiv beraten.

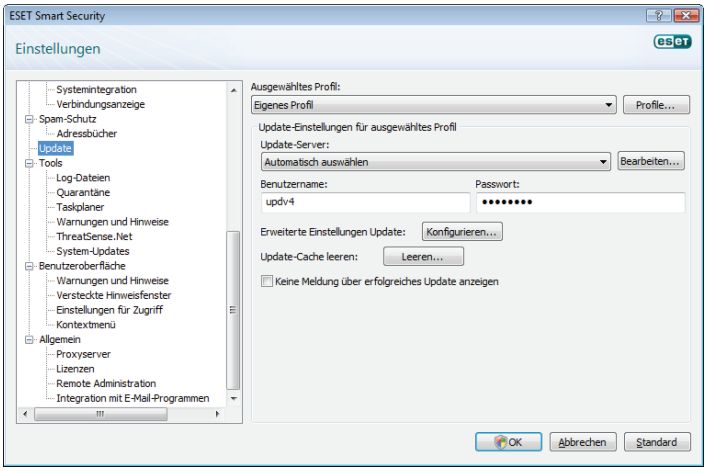
3.2 Einstellungen für Updates

Updates der Signaturdatenbank und Updates von Programmkomponenten sind ein wichtiger Bestandteil der Maßnahmen für einen möglichst umfassenden Schutz vor schädlichem Code. Seien Sie deshalb bei Konfiguration und Ausführung besonders sorgfältig. Wählen Sie im Hauptmenü die Option **Update**, und klicken Sie dann im Hauptprogrammfenster auf **Update der Signaturdatenbank**, um direkt zu überprüfen, ob ein Datenbank-Update verfügbar ist. **Benutzernamen und Passwort festlegen...** öffnet ein Dialogfeld, in dem der beim Kauf erhaltene Benutzername und das Passwort eingegeben werden.

Wenn Benutzername und Passwort bei der Installation von ESET Smart Security eingegeben wurden, werden Sie hier nicht zu einer Eingabe aufgefordert.

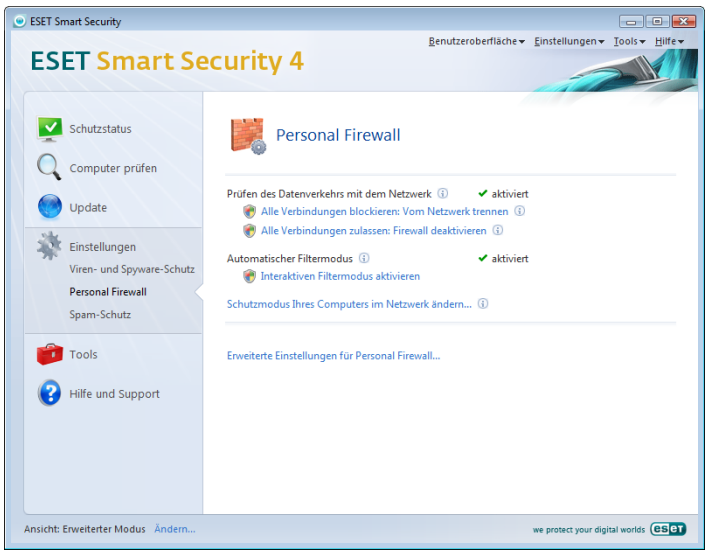


Das (durch Drücken der Taste F5 aufrufbare) Fenster **Erweiterte Einstellungen** enthält weitere Optionen für Updates. Im Dropdown-Menü **Update-Server:** sollte die Option **Automatisch auswählen** ausgewählt sein. Zum Konfigurieren erweiterter Update-Optionen wie Update-Modus, Proxyserverzugriff, Zugriff auf Updates auf einem lokalen Server und Erstellen von Signaturkopien (ESET Smart Security Business Edition) klicken Sie auf **Einstellungen...**.

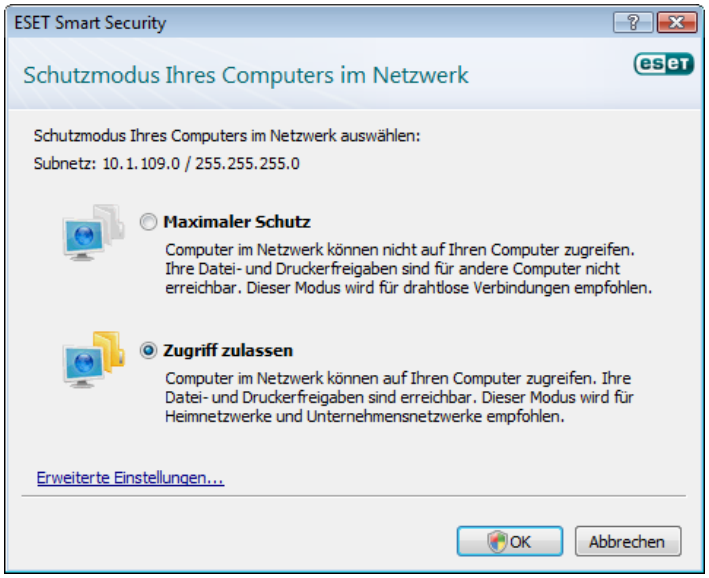


3.3 Einstellungen der vertrauenswürdigen Zone

Die Konfiguration einer vertrauenswürdigen Zone ist ein wichtiges Element für den Schutz von Computern im Netzwerk. Sie können anderen Benutzern Zugriff auf Ihren Computer gewähren, indem Sie die vertrauenswürdige Zone konfigurieren und Freigaben zulassen. Klicken Sie auf **Einstellungen > Personal Firewall > Schutzmodus für Computer im Netzwerk ändern...** Im nun angezeigten Fenster können Sie die Einstellungen für den Computer-Schutzmodus im Netzwerk bzw. in der Zone ändern.



Die Erkennung der vertrauenswürdigen Zone erfolgt nach der Installation von ESET Smart Security und bei jeder neuen Verbindung des Computers mit einem Netzwerk. In den meisten Fällen muss die vertrauenswürdige Zone daher nicht definiert werden. Standardmäßig wird bei Erkennung einer neuen Zone ein Dialogfenster angezeigt, in dem Sie die Schutzstufe für diese Zone festlegen können.

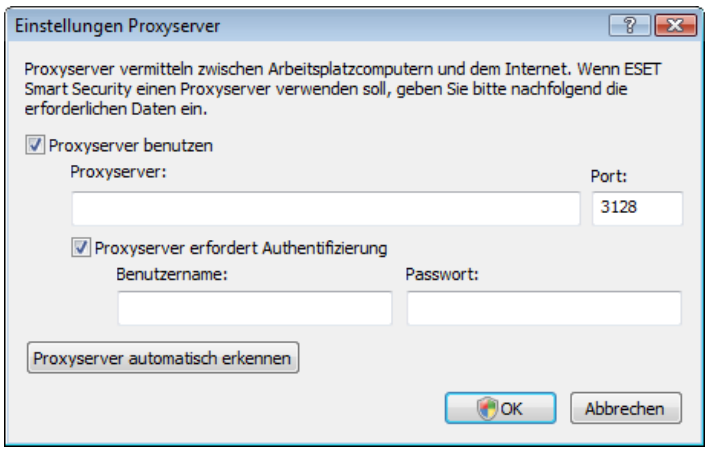

ESET Smart Security
Schutzmodus Ihres Computers im Netzwerk
eset
Schutzmodus Ihres Computers im Netzwerk auswählen:
Subnetz: 10.1.109.0 / 255.255.255.0
Maximaler Schutz
Computer im Netzwerk können nicht auf Ihren Computer zugreifen. Ihre Datei- und Druckerfreigaben sind für andere Computer nicht erreichbar. Dieser Modus wird für drahtlose Verbindungen empfohlen.
Zugriff zulassen
Computer im Netzwerk können auf Ihren Computer zugreifen. Ihre Datei- und Druckerfreigaben sind erreichbar. Dieser Modus wird für Heimnetzwerke und Unternehmensnetzwerke empfohlen.
Erweiterte Einstellungen...
OK
Abbrechen

Warnung! Eine falsche Konfiguration der vertrauenswürdigen Zone kann ein Sicherheitsrisiko für Ihren Computer darstellen.

HINWEIS: Computer innerhalb der vertrauenswürdigen Zone erhalten standardmäßig Zugriff auf freigegebene Dateien und Drucker, die RPC-Kommunikation ist aktiviert und Remotedesktopverbindungen sind ebenfalls möglich.

3.4 Einstellungen für den Proxyserver

Wenn Sie einen Proxyserver nutzen, um die Internetverbindung eines Systems zu vermitteln, auf dem ESET Smart Security verwendet wird, so muss dies in den erweiterten Einstellungen (F5) angegeben werden. Um das Konfigurationsfenster **Proxyserver** zu öffnen, klicken Sie unter „Erweiterte Einstellungen" auf **Allgemein > Proxyserver**. Aktivieren Sie das Kontrollkästchen **Folgenden Proxyserver verwenden**, und geben Sie die IP-Adresse und den Port des Proxyservers sowie die Authentifizierungsdaten ein.



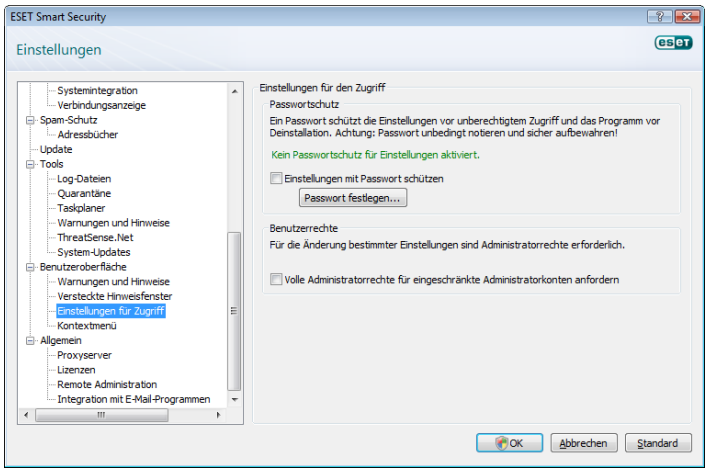
Wenn Ihnen diese Informationen nicht zur Verfügung stehen, können Sie versuchen, die Proxyservereinstellungen für ESET Smart Security automatisch erkennen zu lassen. Dazu klicken Sie auf **Proxyserver automatisch erkennen**.

HINWEIS: Die Proxyserver-Optionen für verschiedene Update-Profile können voneinander abweichen. Konfigurieren Sie den Proxyserver in diesem Fall über die erweiterten Einstellungen für Updates

3.5 Einstellungen schützen

Die Einstellungen von ESET Smart Security können im Hinblick auf die Sicherheitsrichtlinien Ihres Unternehmens von großer Wichtigkeit sein. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Um die Einstellungen mit einem Passwort zu schützen, klicken Sie im Hauptmenü auf **Einstellungen > Erweiterte Einstellungen... > Benutzeroberfläche > Einstellungen schützen**, und klicken Sie auf **Passwort eingeben...**.

Geben Sie ein Passwort ein, und bestätigen Sie es durch erneutes Eingeben. Klicken Sie anschließend auf **OK**. Dieses Passwort ist erforderlich, um künftige Änderungen an den Einstellungen von ESET Smart Security vorzunehmen.



4. Mit ESET Smart Security arbeiten

4.1 Viren- und Spyware-Schutz

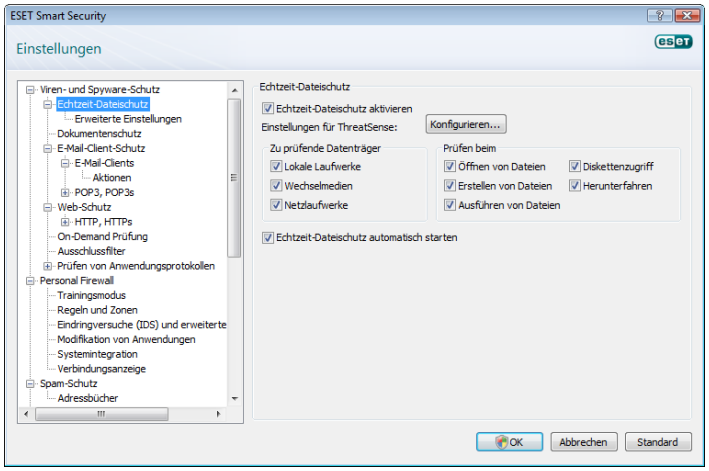
Virenschutzlösungen bieten durch Überwachung der Daten-, E-Mail- und Internet-Kommunikation Schutz vor bösartigen Systemangriffen. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es zunächst die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.

4.1.1 Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle für den Virenschutz relevanten Systemereignisse. Alle Dateien werden beim Öffnen, Erstellen oder Ausführen auf dem Computer auf Schadcode geprüft. Der Echtzeit-Dateischutz wird beim Systemstart gestartet.

4.1.1.1 Prüfeinstellungen

Der Echtzeit-Dateischutz prüft alle Datenträger, wobei die Prüfung von verschiedenen Ereignissen ausgelöst wird. Zum Prüfen werden ThreatSense-Erkennungsmethoden verwendet (siehe „Einstellungen für ThreatSense"). Das Prüfverhalten kann für neu erstellte Dateien und vorhandene Dateien variieren. Neu erstellte Dateien können einer noch gründlicheren Prüfung unterzogen werden.



4.1.1.1.1 Zu prüfende Datenträger

Standardmäßig werden alle Arten von Datenträgern auf mögliche Bedrohungen geprüft.

Lokale Laufwerke – Alle Festplatten des Systems werden geprüft

Wechselmedien – Disketten, USB-Speichergeräte usw.

Netzlaufwerke – Alle verbundenen Netzlaufwerke werden geprüft

Ändern Sie diese Einstellungen nur in Ausnahmefällen, z. B. wenn die Prüfung bestimmter Datenträger die Datenübertragung verlangsamt.

4.1.1.1.2 Prüfen bei Ereignis

Standardmäßig werden alle Dateien beim Öffnen, Ausführen oder Erstellen geprüft. Wir empfehlen Ihnen, die Standardeinstellungen beizubehalten. So verfügen Sie über maximalen Echtzeit-Dateischutz auf Ihrem Computer.

Über die Option **Diskettenzugriff** können Sie den Bootsektor einer Diskette prüfen, wenn auf das entsprechende Laufwerk zugegriffen wird. Über die Option **Herunterfahren** können Sie die Festplatten-Bootsektoren beim Herunterfahren des Computers prüfen. Auch wenn Boot-Viren heutzutage selten sind, sollten Sie diese Optionen dennoch aktivieren, da die Gefahr der Infektion durch einen Boot-Virus aus alternativen Quellen durchaus besteht.

4.1.1.1.3 Zusätzliche ThreatSense-Einstellungen für neu erstellte und geänderte Dateien

Die Wahrscheinlichkeit einer Infektion ist bei neu erstellten oder geänderten Dateien vergleichsweise höher als bei schon länger vorhandenen Dateien. Für die Prüfung dieser Dateien werden daher zusätzliche Parameter herangezogen. Neben gewöhnlichen Prüfmethoden auf Signaturbasis werden erweiterte heuristische Verfahren verwendet, wodurch die Erkennungsrate deutlich steigt. Es werden nicht nur neu erstellte Dateien, sondern auch selbstentpackende Dateien (SFX) und laufzeitkomprimierte Dateien (intern komprimierte ausführbare Dateien) geprüft. Standardmäßig werden Archive bis zur 10. Verschachtelungstiefe gescannt und unabhängig von der tatsächlichen Größe überprüft. Deaktivieren Sie die Option ***Standard-Archivprüfeinstellungen***, um die Einstellungen für das Scannen von Archiven zu ändern.

4.1.1.1.4 Erweiterte Einstellungen

Um die Anzahl der geprüften Objekte möglichst gering zu halten, werden Dateien, die bereits durch den Echtzeit-Dateischutz geprüft wurden, nicht erneut geprüft (außer sie wurden geändert). Dateien werden nach jedem Update der Signaturdatenbank umgehend erneut geprüft. Dieses Verhalten wird über die Option **Optimiertes Prüfen** konfiguriert. Ist diese Option deaktiviert, werden alle Dateien bei jedem Zugriff geprüft.

Der Echtzeit-Dateischutz wird standardmäßig beim Starten des Betriebssystems gestartet und fortlaufend ausgeführt. In Ausnahmefällen (z. B. bei einem Konflikt mit einer anderen Echtzeit-Prüfung) kann die Ausführung des Echtzeit-Dateischutzes abgebrochen werden. Deaktivieren Sie dazu die Option **Echtzeit-Dateischutz automatisch starten**.

Standardmäßig werden die erweiterten Heuristik-Funktionen bei der Ausführung von Dateien nicht verwendet. Dennoch werden Sie diese Option gegebenenfalls in manchen Fällen aktivieren wollen. (Durch das Aktivieren der Option **Erweiterte Heuristik bei Dateiausführung**) Beachten Sie, dass die erweiterten Heuristik-Funktionen die Ausführung einiger Programme durch erhöhte Systemanforderungen verlangsamen können.

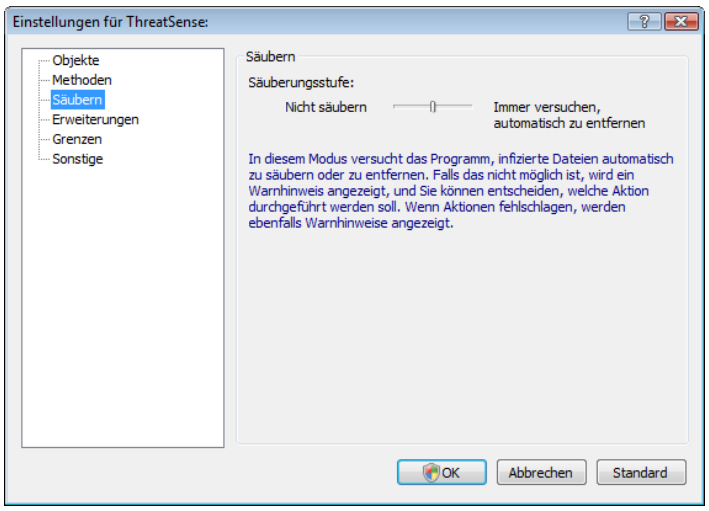
4.1.1.2 Entfernungsstufen

Der Echtzeit-Dateischutz verfügt über drei Entfernungsstufen (um darauf zuzugreifen, klicken Sie im Bereich **Echtzeit-Dateischutz** auf **Einstellungen...**, und wählen Sie dann **Schadcode entfernen**).

- Auf der ersten Entfernungsstufe wird für jede erkannte eingedrungene Schadsoftware eine Warnung angezeigt, die eine Auswahl an Optionen bereitstellt. Der Benutzer muss für jede eingedrungene Schadsoftware eine eigene Aktion auswählen. Diese Stufe eignet sich vor allem für fortgeschrittene Benutzer, die wissen, wie sie bei eingedrungenem Schadcode vorgehen müssen.

- Auf der mittleren Stufe wird automatisch eine vordefinierte Aktion ausgewählt und ausgeführt, je nach Typ der eingedrungenen Schadsoftware. Eine Informationsnachricht am unteren rechten Bildschirmrand informiert über die Erkennung und das Löschen infizierter Dateien. Eine automatische Aktion wird nicht ausgeführt, wenn sich die infizierte Datei in einem Archiv befindet und dieses weitere nicht infizierte Dateien enthält. Gleiches gilt für Objekte, für die keine vordefinierte Aktion angegeben wurde.

- Die dritte Entfernungsstufe ist am „aggressivsten", der Schadcode aller infizierten Objekte wird entfernt. Da hierbei möglicherweise wichtige Dateien verloren gehen, sollten Sie auf diesen Modus nur in besonderen Fällen zurückgreifen.


Einstellungen für ThreatSense:
Objekte
Methoden
Säubern
Erweiterungen
Grenzen
Sonstige
Säubern
Säuberungsstufe:
Nicht säubern
Immer versuchen, automatisch zu entfernen
In diesem Modus versucht das Programm, infizierte Dateien automatisch zu säubern oder zu entfernen. Falls das nicht möglich ist, wird ein Warnhinweis angezeigt, und Sie können entscheiden, welche Aktion durchgeführt werden soll. Wenn Aktionen fehlschlagen, werden ebenfalls Warnhinweise angezeigt.
OK
Abbrechen
Standard

4.1.1.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System. Daher sollte gründlich geprüft werden, ob eine Änderung der Einstellungen wirklich notwendig ist. Es wird empfohlen, nur in einzelnen Fällen die Parameter zu verändern. Es kann beispielsweise erforderlich sein, wenn ein Konflikt mit einer bestimmten Anwendung oder der Echtzeit-Prüfung eines anderen Virenschutzprogramms vorliegt.

Bei der Installation von ESET Smart Security werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Um die Standardeinstellungen wiederherzustellen, klicken Sie auf die Schaltfläche **Standard**, die sich unten rechts im Fenster **Echtzeit-Dateischutz** befindet (**Erweiterte Einstellungen > Viren- und Spyware-Schutz > Echtzeit-Dateischutz**).

4.1.1.4 Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz ordnungsgemäß funktioniert und Viren erkennt, verwenden Sie eine Testdatei von eicar.com. Bei dieser Testdatei handelt es sich um eine spezielle, harmlose Datei, die von allen Virenschutzprogrammen erkannt wird. Die Datei wurde von der Firma EICAR (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen. Die Datei „eicar.com" kann unter http://www.eicar.org/download/eicar.com

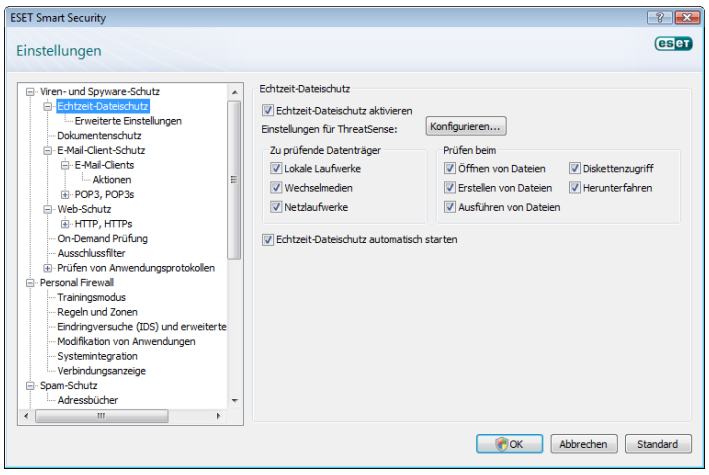
HINWEIS: Bevor Sie eine Prüfung des Echtzeit-Dateischutzes durchführen, müssen Sie die Firewall deaktivieren. Bei aktivierter Firewall wird die Datei erkannt, und die Testdateien können nicht heruntergeladen werden.

4.1.1.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

Im nächsten Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

Echtzeit-Dateischutz ist deaktiviert
Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Dateischutz wieder zu aktivieren, wählen Sie **Einstellungen > Viren- und Spyware-Schutz**, und klicken Sie im Bereich **Echtzeit-Dateischutz** des Hauptprogrammfensters auf **Aktivieren**.

Wenn der Echtzeit-Dateischutz beim Systemstart nicht gestartet wird, liegt das wahrscheinlich daran, dass die Option **Echtzeit-Dateischutz automatisch starten** deaktiviert ist. Um die Option zu aktivieren, wählen Sie **Erweiterte Einstellungen** (F5), und klicken Sie dort auf **Echtzeit-Dateischutz**. Vergewissern Sie sich, dass im Bereich **Erweiterte Einstellungen** im unteren Teil des Fensters das Kontrollkästchen **Echtzeit-Dateischutz automatisch starten** aktiviert ist.



Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode
Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Echtzeit-Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, alle anderen Virenschutzprogramme zu deinstallieren.

Echtzeit-Dateischutz startet nicht
Wenn der Echtzeit-Dateischutz beim Systemstart nicht initialisiert wird (und die Option **Echtzeit-Dateischutz automatisch starten** aktiviert ist), kann das an Konflikten mit anderen Programmen liegen. Sollte dies der Fall sein, wenden Sie sich an einen der Experten des ESET-Kundendienstes.

4.1.2 Host Intrusion Prevention System (HIPS)

Host Intrusion Prevention System (HIPS) schützt Ihr System vor Malware oder anderen unerwünschten Aktivitäten, die die Sicherheit Ihres Computers negativ beeinflussen. Die Kombination aus fortgeschrittener Verhaltensanalyse und der Netzwerküberwachung durch den ESET Webschutz ermöglicht ein Monitoring laufender Prozesse, Dateien sowie der Windows Registrierung und kann unerwünschten Vorgängen vorbeugen und diese blockieren.

4.1.3 E-Mail-Client-Schutz

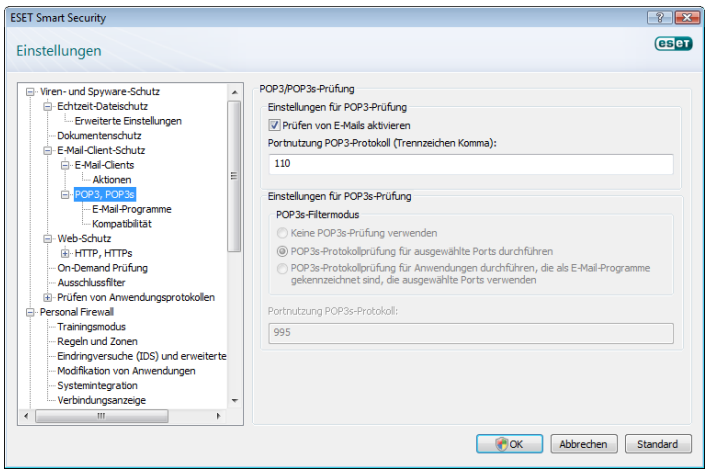
Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3-Protokoll übertragen werden. Mithilfe der Plugin-Software für Microsoft Outlook stellt ESET Smart Security Kontrollfunktionen für die gesamte E-Mail-Kommunikation (POP3, MAPI, IMAP, HTTP) bereit. Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Prüfmethoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Signaturdatenbank statt. Die Prüfung der POP3-Kommunikation erfolgt unabhängig vom verwendeten E-Mail-Programm.

4.1.3.1 POP3-Prüfung

Das POP3-Protokoll ist das am häufigsten verwendete Protokoll zum Empfangen von E-Mail-Nachrichten mit einem E-Mail-Programm. ESET Smart Security bietet POP3-Protokoll-Schutzfunktionen unabhängig vom verwendeten E-Mail-Programm.

Das Modul, das diese Kontrollfunktion bereitstellt, wird automatisch beim Start des Betriebssystems initialisiert und ist dann im Speicher aktiv. Um das Modul einsetzen zu können, muss es aktiviert sein. Die POP3-Prüfung wird automatisch ausgeführt, und das E-Mail-Programm muss nicht neu konfiguriert werden. In der Standardeinstellung wird die gesamte Kommunikation über Port 110 geprüft. Bei Bedarf können weitere Kommunikationsports hinzugefügt werden. Portnummern müssen durch ein Komma voneinander getrennt sein.

Verschlüsselte Kommunikation wird nicht geprüft.



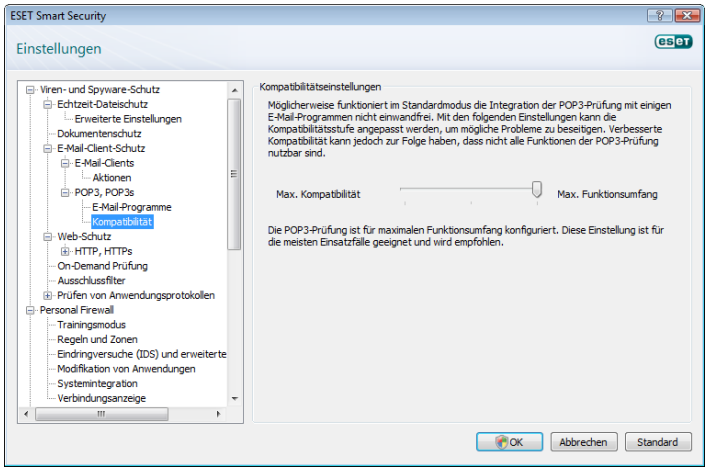
4.1.3.1.1 Kompatibilität

Bei bestimmten E-Mail-Programmen können Probleme mit der POP3-Prüfung auftreten (wenn Sie z. B. eine langsame Internetverbindung verwenden, kann es beim Prüfen zu Zeitüberschreitungen kommen). Sollte dies der Fall sein, ändern Sie die Prüfeinstellungen. Wenn Sie die Prüfmethoden lockern, kann das Entfernen von Schadcode beschleunigt werden. Um die Stufe der POP3-Prüfung anzupassen, wählen Sie **Viren- und Spyware-Schutz > E-Mail-Schutz > POP3 > Kompatibilität**.

Bei Aktivierung der Option **Maximaler Funktionsumfang** wird eingedrungener Schadcode aus infizierten Nachrichten entfernt (wenn die Optionen **Löschen** oder **Entfernen** aktiviert sind oder die Entfernungsstufen **Immer versuchen, automatisch zu entfernen** oder **Standard** aktiviert sind).

Mittlere Kompatibilität ändert die Art und Weise, wie Nachrichten empfangen werden. Nachrichten werden stückweise an das E-Mail-Programm gesendet, und nachdem der letzte Teil der Nachricht übertragen wurde, wird die Nachricht auf Schadcode geprüft. Bei dieser Prüfmethode steigt das Infektionsrisiko. Die Entfernungsstufe und die Behandlung von Prüfhinweisen (Warnhinweise, die an die Betreffzeile und den E-Mail-Nachrichtentext angehängt werden) entsprechen den Einstellungen der Option „Maximaler Funktionsumfang".

Bei der Stufe **Maximale Kompatibilität** wird der Benutzer mithilfe eines Alarmfensters über den Empfang einer infizierten Nachricht informiert. Es werden keine Informationen über infizierte Dateien an die Betreffzeile oder den Text eingegangener Nachrichten angehängt, und eingedrungener Schadcode wird nicht automatisch entfernt. Den Schadcode muss der Benutzer vom E-Mail-Programm aus entfernen.

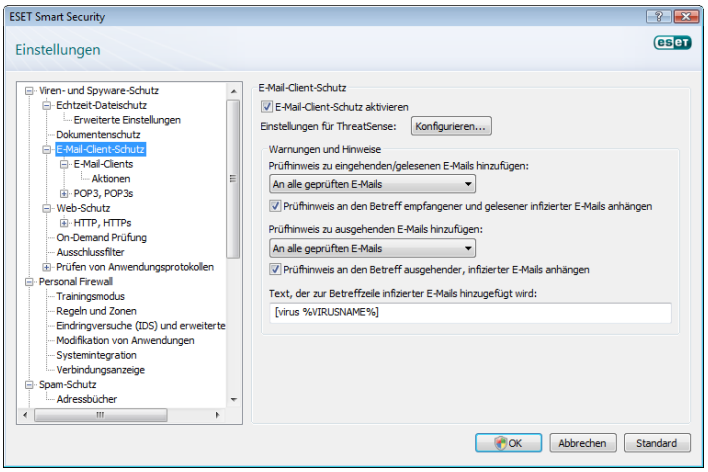


4.1.3.2 Integration in E-Mail-Programme

Die Integration von ESET Smart Security mit E-Mail-Programmen verbessert den aktiven Schutz gegen Schadcode in E-Mail-Nachrichten. Wenn Ihr E-Mail-Programm unterstützt wird, können Sie diese Integration in ESET Smart Security aktivieren. Bei aktivierter Integration wird die Spam-Schutz-Symbolleiste von ESET Smart Security direkt in das E-Mail-Programm eingebunden. Auf diese Weise können E-Mails effizienter geschützt werden. Die Integrationseinstellungen finden Sie unter **Einstellungen > Erweiterte Einstellungen... > Allgemein > Integration mit E-Mail-Programmen**. Über dieses Dialogfeld können Sie die Integration mit den unterstützten E-Mail-Programmen aktivieren. Unter anderem die folgenden E-Mail-Clients werden gegenwärtig unterstützt: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail und Mozilla Thunderbird.

Wählen Sie die Option ***Prüfen neuer Elemente im Posteingang deaktivieren*** aus, wenn Sie bei der Arbeit mit Ihrem E-Mail-Client eine Verlangsamung des Systems feststellen. Dies tritt möglicherweise ein, wenn Sie E-Mails aus Kerio Outlook Connector Store herunterladen.

Der E-Mail-Schutz wird gestartet, indem Sie das Kontrollkästchen **E-Mail-Schutz aktivieren** unter **Erweiterte Einstellungen (F5)** > **Viren- und Spyware-Schutz** > **E-Mail-Schutz aktivieren**.



4.1.3.2.1 E-Mail-Nachrichtentexten Prüfhinweise hinzufügen

An den Betreff oder den Nachrichtentext jeder E-Mail, die von ESET Smart Security überwacht wird, kann ein Prüfhinweis angehängt werden. Diese Funktion erhöht die Glaubwürdigkeit der von einem Benutzer gesendeten Nachrichten. Bei der Erkennung von eingedrungener Schadsoftware stehen hilfreiche Informationen zur Verfügung, um den Bedrohungsgrad durch den Sender einzuschätzen.

Die Optionen für diese Funktion werden unter **Erweiterte Einstellungen > Viren- und Spyware-Schutz > E-Mail-Client-Schutz** festgelegt. Das Programm kann sowohl einen **Prüfhinweis zu eingehenden E-Mails hinzufügen** als auch einen **Prüfhinweis zu ausgehenden E-Mails hinzufügen**. Für beide Optionen kann der Benutzer festlegen, ob jeder E-Mail, nur infizierten E-Mails oder gar keiner E-Mail ein Prüfhinweis angehängt werden soll. Mit ESET Smart Security können Benutzer auch dem Original-Betreff der infizierten Nachrichten Prüfhinweise anhängen. Zum Aktivieren dieser Funktion verwenden Sie die Optionen **Prüfhinweis zum Betreff eingehender E-Mails hinzufügen (nur infizierte E-Mails)** und **Prüfhinweis zum Betreff ausgehender E-Mails hinzufügen (nur infizierte E-Mails)**.

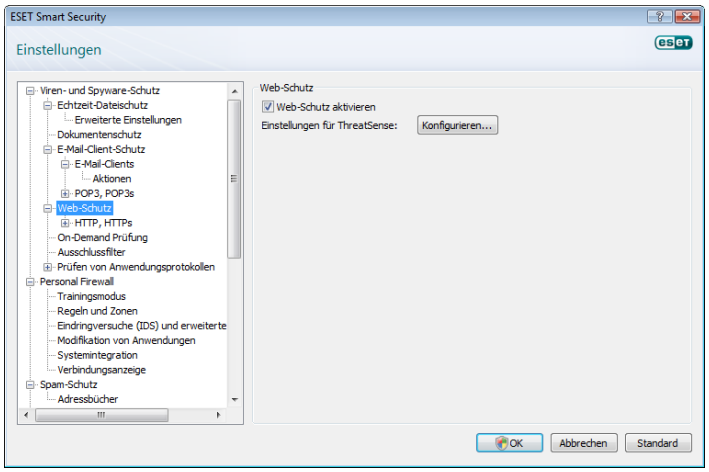
Der Inhalt der Hinweise kann im Feld „Vorlage" bearbeitet und dem Betreff der infizierten E-Mails hinzugefügt werden. Die oben genannten Änderungen dienen dazu, die Filterung infizierter E-Mails zu automatisieren, indem E-Mail-Nachrichten mit einem bestimmten Betreff in einen getrennten Ordner aussortiert werden können (falls von Ihrem E-Mail-Programm unterstützt).

4.1.3.3 Eingedrungene Schadsoftware entfernen

Bei Empfang einer infizierten E-Mail-Nachricht wird eine Warnung angezeigt. Die Warnung enthält den Namen des Absenders, die E-Mail und den Namen der eingedrungenen Schadsoftware. Im unteren Bereich des Fensters können Sie zwischen den Optionen **Säubern**, **Löschen** oder **Belassen** für das entdeckte Objekt auswählen. In fast allen Fällen sollten Sie entweder **Säubern** oder **Löschen** wählen. Um die infizierte Datei in Ausnahmesituationen zu empfangen, wählen Sie **Belassen**. Wenn die Option **Immer versuchen, automatisch zu entfernen** aktiviert ist, wird ein Informationsfenster ohne Auswahloptionen für das infizierte Objekt angezeigt.

4.1.4 Web-Schutz

Die Internetverbindung ist eine Standardfunktion jedes Computers. Doch leider ist sie auch der Hauptübertragungsweg für Schadcode. Daher ist es überaus wichtig, für einen ausreichenden Web-Schutz zu sorgen. Die Option **Web-Schutz aktivieren** sollte in jedem Fall aktiviert werden. Sie finden diese Option unter **Erweiterte Einstellungen (F5) > Viren- und Spyware-Schutz > Web-Schutz**.



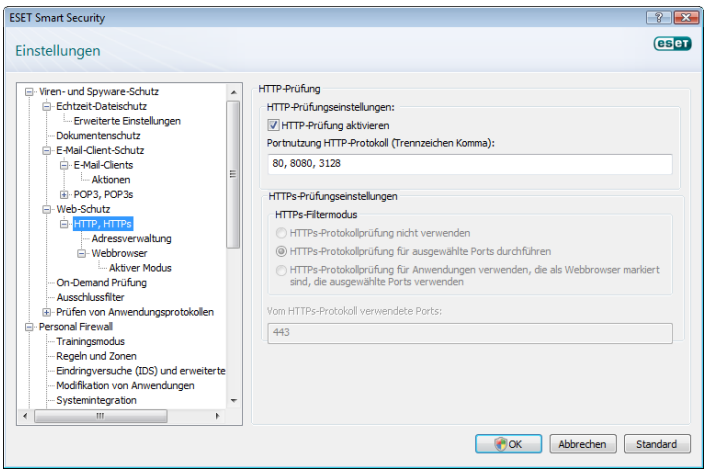
4.1.4.1 HTTP, HTTPs

Der Web-Schutz funktioniert durch die Überwachung der Kommunikation zwischen Webbrowsern und Remote-Servern und erfüllt die HTTP-Regeln (Hypertext Transfer Protocol) und die HTTPs-Regeln (verschlüsselte Kommunikation). Standardmäßig ist ESET Smart Security für die Verwendung der Standards der gängigen Webbrowser konfiguriert. Die HTTP-Prüfungseinstellungsoptionen können jedoch unter Web-Schutz > HTTP, HTTPs geändert werden. Im HTTP-Filter-Hauptfenster können Sie die Option **HTTP-Prüfung aktivieren** aktivieren oder deaktivieren. Sie können auch die für die HTTP-Kommunikation verwendeten Portnummern definieren. In der Standardeinstellung sind die Portnummern 80, 8080 und 3128 vorgegeben. Die HTTPs-Prüfung kann in den folgenden Modi ausgeführt werden:

HTTPs-Protokollprüfung nicht verwenden
Die verschlüsselte Kommunikation wird nicht geprüft.

HTTPs-Protokollprüfung für ausgewählte Ports durchführen
Die HTTPs-Prüfung erfolgt ausschließlich für die unter "Vom HTTPs-Protokoll verwendete Ports" definierten Ports.

HTTPs-Protokollprüfung für Anwendungen verwenden, die als Webbrowser markiert sind, die ausgewählte Ports verwenden
Aktivieren Sie nur Anwendungen, die im Browserabschnitt angegeben sind und die unter ***Vom HTTPs-Protokoll verwendete Ports***.

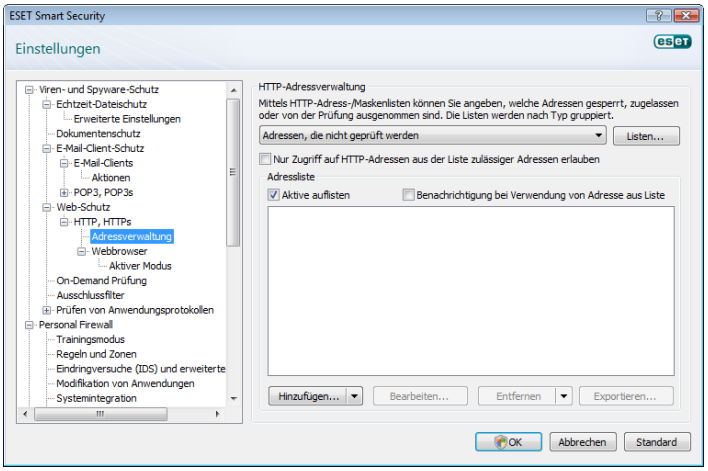


4.1.4.1.1 Adressverwaltung

Dieser Abschnitt ermöglicht es Ihnen, HTTP-Adressen zu spezifizieren, die für die Prüfung blockiert, zugelassen oder ausgeschlossen werden.

Die Schaltflächen **Hinzufügen, Ändern, Entfernen** und **Exportieren** werden zur Verwaltung der Adressenlisten verwendet. Auf Websites in der Liste der blockierten Adressen kann nicht zugegriffen werden. Auf Websites in der Liste der ausgeschlossenen Adressen wird zugegriffen, ohne dass diese auf Schadcodes überprüft werden. Wenn Sie die Option ***Nur Zugriff auf HTTP-Adressen aus der Liste zulässiger Adressen erlauben*** auswählen, wird nur auf Adressen in der Liste zulässiger Adressen zugegriffen, während andere HTTP-Adressen blockiert werden.

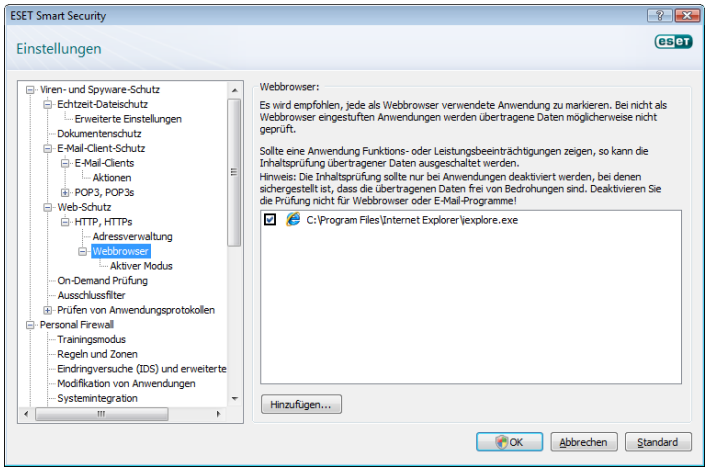
In allen Listen können die Sonderzeichen * (Sternchen) und ? (Fragezeichen) verwendet werden. Das Sternchen ersetzt eine beliebige Zeichenfolge, das Fragezeichen ein beliebiges Symbol. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden. Um eine Liste zu aktivieren, wählen Sie die Option ***Liste aktiv*** aus. Wenn Sie benachrichtigt werden möchten, wenn Sie eine Adresse aus der gegenwärtigen Liste eingeben, wählen Sie die Option ***Benachrichtigung bei Verwendung von Adresse aus Liste***



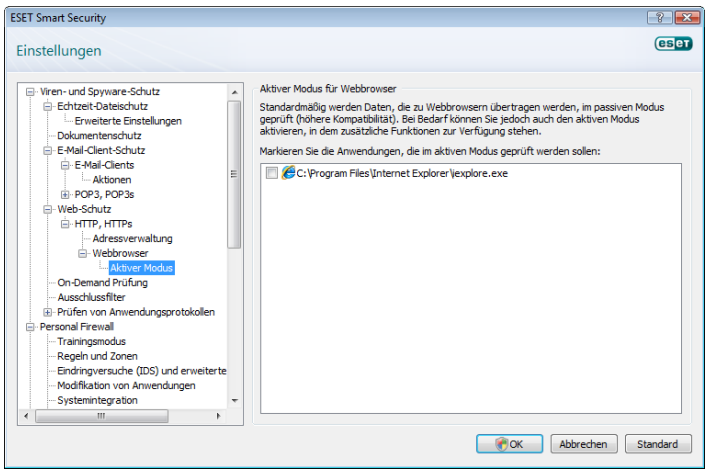
4.1.4.1.2 Webbrowser

Über die Funktion **Webbrowser** von ESET Smart Security kann festgelegt werden, ob es sich bei einer bestimmten Anwendung um einen Browser handelt oder nicht. Wird eine Anwendung vom Benutzer als Browser eingestuft, wird die gesamte Kommunikation dieser Anwendung überwacht, und zwar unabhängig von den verwendeten Portnummern.

Die Webbrowser-Funktion ist eine Ergänzung der HTTP-Prüfung, da die HTTP-Prüfung nur für ausgewählte Ports durchgeführt wird. Viele Internetdienste verwenden jedoch sich dynamisch ändernde oder unbekannte Portnummern. Um diesem Sachverhalt Rechnung zu tragen, kann mithilfe der Webbrowser-Funktion die gesamte Portkommunikation unabhängig von den Verbindungsparametern überwacht werden.



Die Liste der Anwendungen, die als Browser eingestuft sind, kann im Bereich **HTTP** direkt über das Untermenü **Webbrowser** aufgerufen werden. Dieser Abschnitt enthält außerdem das Untermenü **Aktiver Modus**, in dem der Prüfungsmodus für die Webbrowser festgelegt wird. Die Funktion **Aktiver Modus** dient der Untersuchung der übertragenen Daten als Ganzes. Ist die Option nicht aktiviert, wird die Kommunikation der Anwendungen nur Stück für Stück überwacht. Dies verringert die Effizienz der Datenverifizierung, erhöht jedoch die Kompatibilität der aufgeführten Anwendungen. Wenn bei seiner Verwendung keine Probleme auftreten, sollten Sie den aktiven Modus aktivieren, indem Sie das Kontrollkästchen neben der gewünschten Anwendung aktivieren.



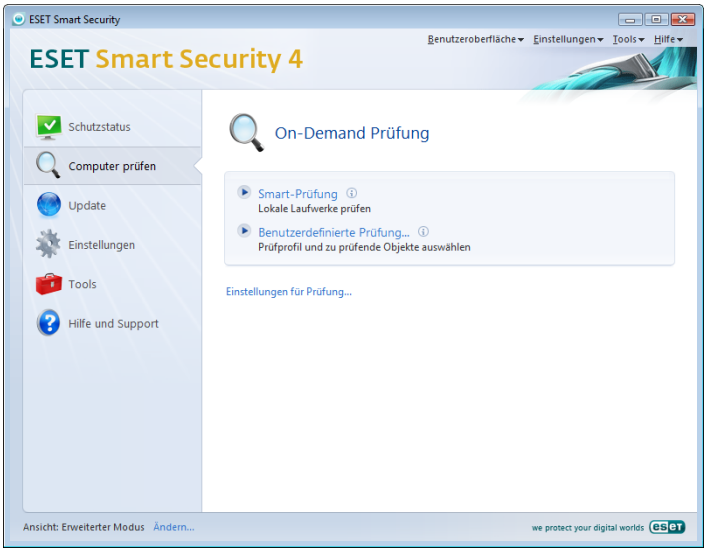
4.1.5 Computer prüfen

Wenn Sie den Verdacht haben, dass Ihr Computer infiziert ist (anormales Verhalten), führen Sie eine manuelle Prüfung aus, um Ihren Computer auf eingedrungene Schadsoftware zu untersuchen. Aus Sicherheitsgründen ist es dringend erforderlich, dass Sie Ihren Computer nicht nur bei Infektionsverdacht prüfen, sondern diese Prüfung in die allgemeinen Sicherheitsroutinen integrieren. Eine regelmäßige Prüfung dient der Erkennung von eingedrungener Schadsoftware, die vom Echtzeit-Dateischutz zum Zeitpunkt der Speicherung der Schadsoftware nicht erkannt wurde. Dies kommt z. B. vor, wenn die Echtzeit-Prüfung zum Zeitpunkt der Infektion deaktiviert war oder die Signaturdatenbank nicht auf dem neuesten Stand ist.

Sie sollten mindestens ein- bis zweimal im Monat eine manuelle Prüfung vornehmen. Sie können die Prüfung als Task unter **Extras > Taskplaner** konfigurieren.

4.1.5.1 Prüfmethode

Es stehen zwei Methoden zur Auswahl. Bei der **Standardprüfung** wird das System schnell überprüft, ohne dass Sie dafür weitere Prüfparameter konfigurieren müssen. Bei der Methode **Prüfen mit speziellen Einstellungen**... können Sie eines der vordefinierten Prüfprofile auswählen und die zu prüfenden Objekte in der Baumstruktur auswählen.



4.1.5.1.1 Standardprüfung

Die Standardprüfung ist eine benutzerfreundliche Methode, mit der Benutzer einen Computer schnell prüfen und infizierte Dateien ohne weiteres Eingreifen entfernen können. Die Bedienung ist einfach, und es ist keine ausführliche Konfiguration erforderlich. Bei der Standardprüfung werden alle Dateien auf den lokalen Laufwerken geprüft, und erkannte eingedrungene Schadsoftware wird automatisch entfernt oder gelöscht. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Entfernungstypen finden Sie unter „Schadcode entfernen“ (siehe Seite 18).

Das Standardprofil ist für Benutzer gedacht, die ihren Computer schnell und einfach auf Viren prüfen möchten. Die Prüfung des Computers und das Entfernen der Schadsoftware mit dem Standardprofil sind effizient und erfordern keine ausführliche Konfiguration.

4.1.5.1.2 Prüfen mit speziellen Einstellungen

Über die Option „Prüfen mit speziellen Einstellungen“ können Sie Prüfparameter wie die zu prüfenden Objekte oder Prüfmethoden angeben. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Die Konfigurationen können in benutzerdefinierten Prüfprofilen gespeichert werden, die sinnvoll sind, wenn Prüfungen wiederholt mit denselben Parametern ausgeführt werden.

Um die zu prüfenden Objekte auszuwählen, verwenden Sie das Dropdown-Menü der Ziel-Schnellauswahl, oder wählen Sie die Objekte in der Baumstruktur aus, in der alle auf dem Computer verfügbaren Geräte aufgeführt werden. Außerdem können Sie zwischen drei Entfernungsstufen wählen. Klicken Sie dazu auf **Einstellungen... > Schadcode entfernen**. Wenn Sie das System ohne zusätzliche Aktionen prüfen möchten, wählen Sie die Option **Nur prüfen, keine Aktion**.

Das Prüfen mit speziellen Einstellungen eignet sich für fortgeschrittene Benutzer, die bereits Erfahrung mit Virenschutzprogrammen gesammelt haben.

4.1.5.2 Zu prüfende Objekte

Über das Dropdown-Menü „Zu prüfende Objekte" werden die Dateien, Ordner und Geräte (Laufwerke) ausgewählt, die auf Viren geprüft werden sollen.

Über die Menüoption „Zu prüfende Objekte" können Sie die folgenden Objekte festlegen:

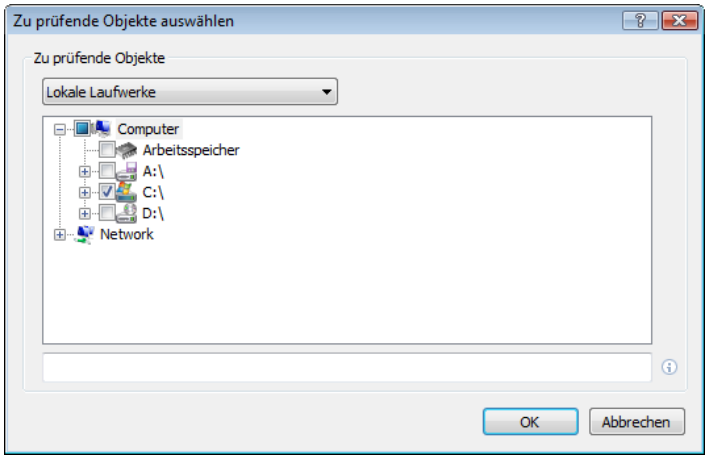
Nach Profileinstellungen – Steuert Ziele, die im ausgewählten Prüfprofil eingestellt sind

Wechselmedien – Disketten, USB-Speichergeräte, CD/DVD

Lokale Laufwerke – Alle Festplatten des Systems werden geprüft

Netzlaufwerke – Alle verbundenen Netzlaufwerke

Keine Auswahl – Hebt jede Auswahl auf



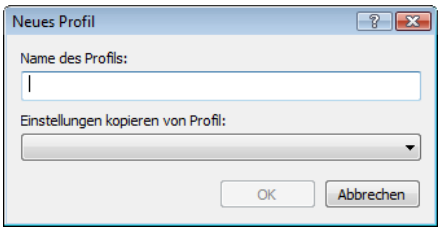
Sie können ein zu prüfendes Objekt auch genauer angeben, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die geprüft werden sollen. Wählen Sie die zu prüfenden Objekte aus der Baumstruktur aus, in der alle auf dem Computer verfügbaren Geräte aufgelistet werden.

4.1.5.3 Prüfprofile

Die bevorzugten Parameter zum Prüfen Ihres Computers können als Profil gespeichert werden. Durch das Erstellen von Prüfprofilen können Sie dieselben Parameter in Zukunft regelmäßig wiederverwenden. Wir empfehlen Ihnen, nur solche Profile (mit verschiedenen zu prüfenden Objekten, Prüfmethoden und anderen Parametern) zu erstellen, die der Benutzer auch regelmäßig verwendet.

Um ein neues Profil zu erstellen, das wiederholt für Prüfungen eingesetzt werden kann, wählen Sie **Erweiterte Einstellungen** (F5) **> Manuelles Prüfen des Computers**. Klicken Sie rechts auf die Schaltfläche **Profile...**, um die Liste vorhandener Prüfprofile anzuzeigen, und anschließend auf die Option zum Erstellen eines neuen Profils. Die folgenden **Einstellungen für ThreatSense** beschreiben jeden Parameter der Prüfeinstellungen. Auf diese Weise können Sie ein Prüfprofil erstellen, das Ihren Anforderungen gerecht wird.

Beispiel:
Angenommen, Sie möchten Ihr eigenes Prüfprofil erstellen und halten die Konfiguration des Profils **Smart Scan** für teilweise geeignet. Sie möchten jedoch keine laufzeitkomprimierten Dateien oder potenziell unsicheren Anwendungen prüfen. Außerdem möchten Sie die Option **Immer versuchen, automatisch zu entfernen** anwenden. Klicken Sie im Fenster **Konfigurationsprofile** auf **Hinzufügen...**. Geben Sie den Namen des neuen Profils im Feld **Profilname** ein und wählen Sie **Smart Scan** aus dem **Einstellungen kopieren von Profil:** Dropdown-Menü aus. Passen Sie anschließend die übrigen Parameter Ihren eigenen Erfordernissen an.



4.1.6 Prüfen von Anwendungsprotokollen

Der Virenschutz für die Anwendungsprotokolle POP3 und HTTP erfolgt mit ThreatSense. Alle erweiterten Prüfmethoden sind in dieses System integriert. Die Prüfung ist unabhängig vom eingesetzten E-Mail-Programm und Webbrowser. Für das Prüfen von Anwendungsprotokollen sind die folgenden Optionen verfügbar (wenn die Option **Prüfen von Anwendungsprotokollen aktivieren** aktiviert ist:

HTTP- und POP3-Ports – beschränkt die Prüfung der Kommunikation auf bekannte HTTP- und POP3-Ports.

Anwendungen, die als Internet-Browser und E-Mail-Clients gekennzeichnet sind – Aktivieren Sie diese Option, um ausschließlich die Kommunikation von Anwendungen zu prüfen, die als Browser (Web-Schutz > HTTP, HTTPS > Webbrowser) und E-Mail-Clients (E-Mail-Client-Schutz > POP3, POP3S > E-Mail-Clients) gekennzeichnet sind.

Ports und Anwendungen, die als Internet-Browser oder E-Mail-Clients gekennzeichnet sind – sowohl Ports als auch Browser werden auf Malware überprüft.

Hinweis:
Ab Windows Vista Service Pack 1 und Windows Server 2008 wird eine neue Kommunikationsprüfung genutzt. Daher steht der Abschnitt für das Prüfen von Anwendungsprotokollen nicht zur Verfügung

4.1.6.1 SSL

ESET Smart Security 4 ermöglicht es Ihnen, die Protokolle zu prüfen, die im SSL-Protokoll gekapselt sind. Sie können verschiedene Prüfmodi für SSL-geschützte Verbindungen verwenden, die vertrauenswürdige Zertifikate, unbekannte Zertifikate oder Zertifikate nutzen, die von der Prüfung SSL-geschützter Verbindungen ausgeschlossen sind.

SSL-Protokoll immer prüfen (ausgeschlossene und vertrauenswürdige Zertifikate bleiben gültig) – Wählen Sie diese Option aus, um alle SSL-geschützten Verbindungen mit Ausnahme der Verbindungen zu prüfen, die durch Zertifikate geschützt werden, die von der Prüfung ausgeschlossen sind. Wenn eine neue Verbindung hergestellt wird, für die ein unbekanntes, signiertes Zertifikat verwendet wird, wird der Benutzer darüber nicht benachrichtigt und die Verbindung wird automatisch geprüft. Wenn der Benutzer auf einen Server mit einem nicht vertrauenswürdigen Zertifikat zugreift, das vom Benutzer als vertrauenswürdig gekennzeichnet ist (es wird zur Liste der vertrauenswürdigen Zertifikate hinzugefügt), dann wird die Verbindung mit dem Server zugelassen und der Inhalt des Verbindungskanals wird geprüft.

Bei nicht besuchten Websites nachfragen (unbekannte Zertifikate)–Wenn Sie eine neue SSL-geschützte Website besuchen (mit unbekanntem Zertifikat), wird ein Auswahldialogfeld angezeigt. Dieser Modus erlaubt es Ihnen, eine Liste von SSL-Zertifikaten zu erstellen, die von der Prüfung ausgeschlossen werden.

SSL-Protokoll nicht prüfen–Wenn dies ausgewählt ist, werden SSL-Verbindungen durch das Programm nicht geprüft.

Wenn das Zertifikat nicht über den Speicher vertrauenswürdiger Stammzertifizierungsstellen geprüft werden kann

Gültigkeit des Zertifikats erfragen–Fordert den Benutzer auf, eine Aktion auszuwählen.

Kommunikation blockieren, die das Zertifikat verwendet–Beendet Verbindung zur Website, die das Zertifikat verwendet.

Wenn das Zertifikat ungültig oder beschädigt ist

Gültigkeit des Zertifikats erfragen–Fordert den Benutzer auf, eine Aktion auszuwählen.

Kommunikation blockieren, die das Zertifikat verwendet–Beendet Verbindung zur Website, die das Zertifikat verwendet.

4.1.6.1.1 Vertrauenswürdige Zertifikate

Neben dem integrierten Speicher der vertrauenswürdigen Stammzertifizierungsstellen, in dem ESET Smart Security 4 vertrauenswürdige Zertifikate speichert, können Sie eine benutzerdefinierte Liste mit vertrauenswürdigen Zertifikaten erstellen, die unter **Einstellungen** (F5) **> Prüfen von Anwendungsprotokollen > SSL > Vertrauenswürdige Zertifikate** angezeigt werden kann.

4.1.6.1.2 Ausgeschlossene Zertifikate

Der Abschnitt der ausgeschlossenen Zertifikate enthält Zertifikate, die als sicher gelten. Das Programm prüft keine Inhalte von verschlüsselten Verbindungen, bei denen Zertifikate aus dieser Liste genutzt werden. Wir empfehlen, nur die Web-Zertifikate zu installieren, die garantiert sicher sind und keine Inhaltsprüfung erfordern.

4.1.7 Einstellungen für ThreatSense

ThreatSense ist eine Technologie, die verschiedene Methoden zur Erkennung von Bedrohungen verwendet. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Stunden eines neuen Angriffs. Eingesetzt wird eine Kombination verschiedener Methoden (Code-Analyse, Code-Emulation, allgemeine Signaturen, Virussignaturen), die zusammen die Systemsicherheit deutlich erhöhen. Die Prüf-Engine kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. Die ThreatSense-Technologie entfernt auch Rootkits erfolgreich.

In den Einstellungen für ThreatSense kann der Benutzer verschiedene Prüfparameter festlegen:

- Dateitypen und -erweiterungen, die geprüft werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

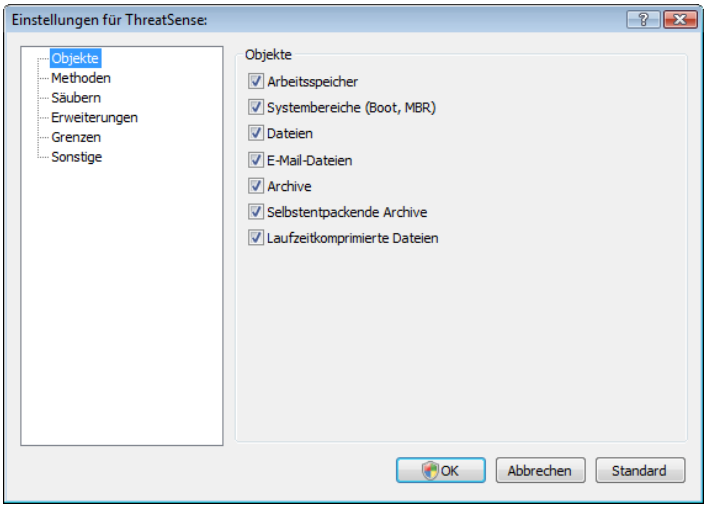
Um das Fenster für die Einstellungen zu öffnen, klicken Sie auf die Schaltfläche **Einstellungen...**, die im Fenster aller Module, die ThreatSense verwenden, angezeigt wird (siehe unten). Je nach Anforderung sind eventuell verschiedene Sicherheitseinstellungen erforderlich. Dies sollte bei den individuellen ThreatSense-Einstellungen für die folgenden Schutzmodule berücksichtigt werden:

- Echtzeit-Dateischutz
- Prüfung Systemstartdateien
- E-Mail-Schutz
- Web-Schutz
- Manuelles Prüfen des Computers

Die ThreatSense-Parameter sind für jedes Modul optimal eingerichtet, und eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Prüfen laufzeitkomprimierter Dateien oder die Aktivierung der erweiterten Heuristik im Modul Echtzeit-Dateischutz dazu führen, dass das System langsamer arbeitet (normalerweise werden mit diesen Methoden nur neu erstellte Dateien geprüft). Es wird daher empfohlen, die Standard-Parameter für ThreatSense in allen Modulen unverändert beizubehalten. Änderungen sollten nur im Modul „Prüfen des Computers" vorgenommen werden.

4.1.7.1 Einstellungen für zu prüfende Objekte

Im Bereich **Objekte** können Sie festlegen, welche Computerkomponenten und Dateien auf Schadcode geprüft werden sollen.



Arbeitsspeicher – Prüfung des Arbeitsspeichers auf mögliche Bedrohungen

Boots-Sektoren – Prüfung der Boot-Sektoren auf Viren im Master Boot Record

Dateien – Prüfung der gängigen Dateitypen (Programm-, Bild-, Audio-, Video-, Datenbankdateien usw.)

E-Mail-Dateien – Prüfung von Dateien, die E-Mail-Nachrichten enthalten

Archive – Prüfung von komprimierten Archivdateien (.rar, .zip, .arj, .tar usw.)

Selbstentpackende Archive – Prüfung von Dateien in selbstentpackenden Archiven; liegen in der Regel mit der Erweiterung .exe vor.

Laufzeitkomprimierte Dateien – Laufzeitkomprimierte Dateien (anders als Standard-Archivtypen) werden im Arbeitsspeicher dekomprimiert, zusätzlich zu statisch laufzeitkomprimierten Dateien (UPX, yoda, ASPack, FGS etc.).

4.1.7.2 Optionen

Im Bereich „Optionen" können Sie die Methoden für die System-Schadsoftwareprüfung auswählen. Folgende Optionen stehen zur Verfügung:

Signaturen – Mit Hilfe von Signaturen kann Schadsoftware zuverlässig anhand des Namens erkannt und identifiziert werden.

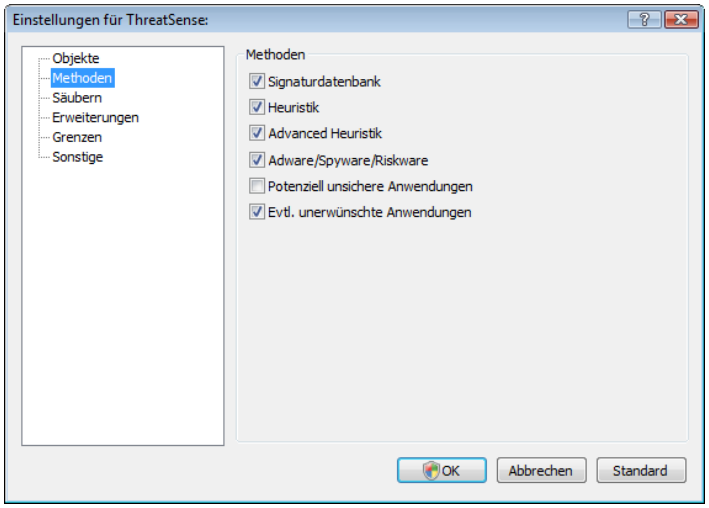
Heuristik – Als heuristische Methoden werden Verfahren bezeichnet, die (bösartige) Aktivitäten von Programmen analysieren. Mit ihrer Hilfe können bis dato unbekannte bösartige Programme oder Viren, die bisher nicht in der Liste bekannter Viren (Signaturdatenbank) aufgeführt waren, erkannt werden.

Advanced Heuristik – Als erweiterte Heuristik werden besondere heuristische Verfahren bezeichnet, die von ESET entwickelt wurden, um Würmer und Trojaner zu erkennen, die in höheren Programmiersprachen geschrieben wurden. Dank erweiterter Heuristik-Funktionen werden die Erkennungsmethoden noch ausgefeilter.

Adware/Spyware/Riskware – Diese Kategorie umfasst Software zum Ausspionieren von vertraulichen Benutzerinformationen. Dazu zählt auch Software zum Anzeigen von Werbebannern.

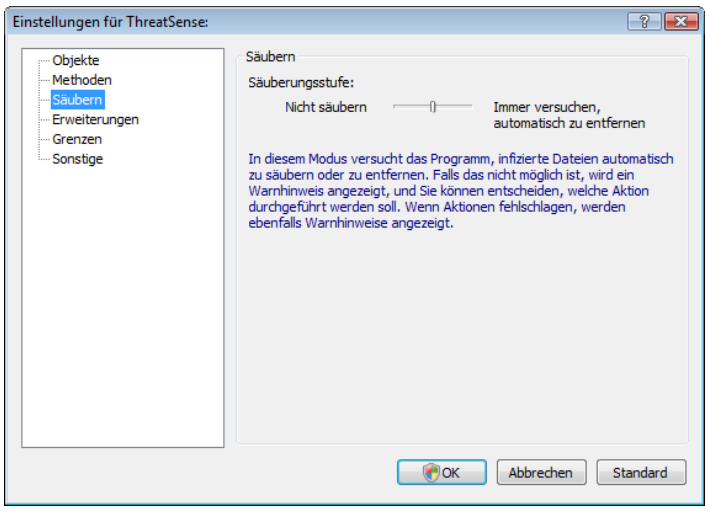
Potenziell unsichere Anwendungen – Unter dieser Bezeichnung werden Programme zusammengefasst, die zwar erwünscht sind, aber Funktionen bereitstellen, die potenziell gefährlich sein können. Da hierzu auch Programme für das Fernsteuern von Computern gehören, ist diese Option standardmäßig deaktiviert.

Eventuell unerwünschte Anwendungen – Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die nicht unbedingt Sicherheitsrisiken mit sich bringen, aber Auswirkungen auf Leistung und Verhalten Ihres Computers haben. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Stand vor der Installation). Dazu zählen vor allem ungewollte Popup-Fenster, die Aktivierung und Ausführung versteckter Prozesse, die erhöhte Inanspruchnahme von Systemressourcen, Änderungen in Suchergebnissen sowie die Kommunikation von Anwendungen mit Remote-Servern.



4.1.7.3 Schadcode entfernen

Die Einstellungen zum Entfernen von Schadcode legen fest, wie beim Entfernen vorgegangen werden soll. Es gibt 3 Arten der Schadcodeentfernung:


Einstellungen für ThreatSense:
Objekte
Methoden
Säubern
Erweiterungen
Grenzen
Sonstige
Säubern
Säuberungsstufe:
Nicht säubern
Immer versuchen, automatisch zu entfernen
In diesem Modus versucht das Programm, infizierte Dateien automatisch zu säubern oder zu entfernen. Falls das nicht möglich ist, wird ein Warnhinweis angezeigt, und Sie können entscheiden, welche Aktion durchgeführt werden soll. Wenn Aktionen fehlschlagen, werden ebenfalls Warnhinweise angezeigt.
OK
Abbrechen
Standard

Schadcode nicht entfernen
Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und der Benutzer wird aufgefordert, eine Aktion auszuwählen.

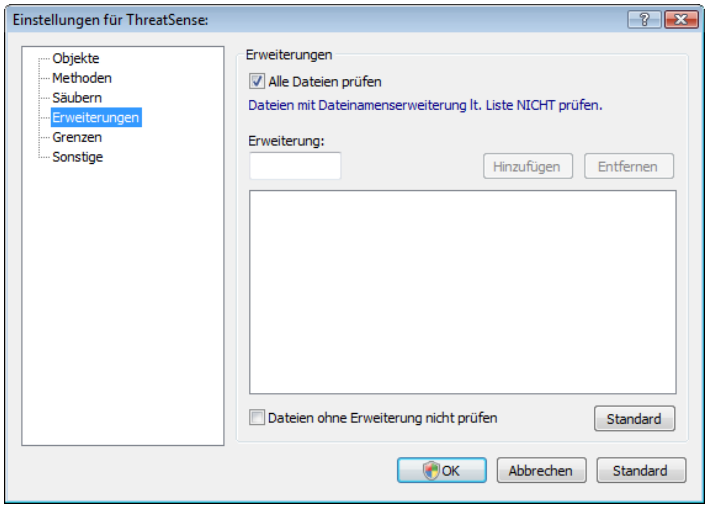
Standardmodus
Das Programm versucht, den Schadcode aus der Datei zu entfernen oder die infizierte Datei zu löschen. Wenn es nicht möglich ist, die angemessene Aktion automatisch zu bestimmen, wird der Benutzer aufgefordert, eine Aktion auszuwählen. Diese Auswahl wird dem Benutzer auch dann angezeigt, wenn eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden konnte.

Immer versuchen, automatisch zu entfernen
Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht die Dateien (einschließlich Archiven). Ausnahmen gelten nur für Systemdateien. Wenn es nicht möglich ist, den Schadcode zu entfernen, wird der Benutzer aufgefordert, eine Aktion auszuwählen.

Warnung:
Im Standardmodus wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Wenn es auch nicht infizierte Dateien enthält, wird die Archivdatei nicht gelöscht. Wenn die Option „Immer versuchen, automatisch zu entfernen" aktiviert ist, wird die Archivdatei gelöscht, sobald eine einzige Datei im Archiv infiziert ist.

4.1.7.4 Dateierweiterungen

Die Erweiterung ist der Teil des Dateinamens nach dem Punkt. Die Erweiterung definiert den Typ und den Inhalt der Datei. In diesem Abschnitt der ThreatSense-Einstellungen legen Sie die Dateitypen fest, die geprüft werden sollen.



In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung geprüft. Jede Erweiterung kann der Liste ausgeschlossener Dateien hinzugefügt werden. Wenn die Option **Alle Dateien prüfen** nicht aktiviert ist, werden in der Liste alle gegenwärtig geprüften Dateierweiterungen angezeigt. Über die Schaltflächen **Hinzufügen** und **Entfernen** können Sie festlegen, welche Erweiterungen geprüft werden sollen.

Um die Prüfung von Dateien ohne Erweiterung zu aktivieren, aktivieren Sie die Option **Dateien ohne Erweiterung prüfen**.

Der Ausschluss bestimmter Dateien ist dann angebracht, wenn die Prüfung bestimmter Dateitypen zu Fehlern bei der Ausführung der zuständigen Programme führt. So sollten Sie z. B. die Erweiterungen „.edb", „.eml" und „.tmp" ausschließen, wenn Sie MS Exchange Server verwenden.

4.1.7.5 Grenzen

Im Abschnitt für die Grenzen können Sie die maximale Größe von Objekten und die maximalen Verschachtelungsstufen von Archiven festlegen, die geprüft werden sollen.

Maximale Objektgröße (Byte)
Definiert die maximale Größe von zu prüfenden Objekten. Das gegebene Virenschutz-Modul prüft anschließend nur Objekte, die kleiner sind als die festgelegte Größe. Wir raten davon ab, den Standardwert zu ändern, da normalerweise kein Grund für eine entsprechende Änderung besteht. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, größere Objekte von der Prüfung auszuschließen.

Maximale Prüfzeit pro Objekt (Sek.)
Definiert den maximalen Zeitwert für die Prüfung eines Objekts. Wenn ein benutzerdefinierter Wert hier eingegeben wurde, beendet das Virenschutz-Modul die Prüfung eines Objekts, wenn die Zeit abgelaufen ist, unabhängig davon, ob die Prüfung abgeschlossen ist.

Verschachtelungstiefe bei Archiven
Legt die maximale Tiefe der Archivprüfung fest. Wir raten davon ab, den Standardwert von 10 zu ändern. Unter normalen Umständen sollte kein Grund für eine Änderung bestehen. Wenn die Prüfung aufgrund der Zahl der Archivverschachtelungen vorzeitig beendet wird, bleibt das Archiv ungeprüft.

Maximalgröße von Dateien im Archiv (Bytes)
Über diese Option können Sie die maximale Dateigröße der Dateien (beim Extrahieren) festlegen, die in zu prüfenden Archiven enthalten sind. Wenn die Prüfung eines Archivs aus diesem Grund vorzeitig beendet wird, bleibt das Archiv ungeprüft.

4.1.7.6 Sonstiges

Alternative Datenströme (ADS) prüfen
Bei den von NTFS-Dateisystemen verwendeten alternativen Datenströmen (ADS) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Prüftechniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

Hintergrundprüfungen mit geringer Priorität ausführen
Jede Prüfung nimmt eine bestimmte Menge von Systemressourcen in Anspruch. Wenn Sie mit Programmen arbeiten, die einen größeren Teil der Systemressourcen beanspruchen, können Sie eine Hintergrundprüfung mit geringer Priorität aktivieren, um für die Anwendungen benötigte Ressourcen zu sparen.

Alle Objekte in Log aufnehmen
Wenn Sie diese Option aktivieren, werden alle geprüften Dateien im Log eingetragen. Es werden also auch Dateien eingetragen, bei denen keine Bedrohung erkannt wurde.

Datum für 'Geändert am' beibehalten
Aktivieren Sie diese Option, um die ursprüngliche Zugriffszeit geprüfter Dateien beizubehalten, statt diese zu aktualisieren (z. B. für die Verwendung bei Datensicherungssystemen).

Smart Optimization
Smart Optimization wurde entwicklelt, um die Effektivität der Überwachung des Systems zu erhöhen. Wenn aktiviert, wird die Scangeschwindigkeit verbessert, ohne die Erkennungsrate oder die Sicherheit des Systems zu beeinträchtigen.

Bildlauf für Log
Mit dieser Option können Sie den Bildlauf für das Log aktivieren oder deaktivieren. Wenn der Bildlauf aktiviert ist, werden die Informationen im Anzeigefenster nach oben verschoben.

Hinweis zum Abschluss der Prüfung in separatem Fenster anzeigen
Es wird ein separates Fenster mit den Informationen über die Prüfergebnisse angezeigt.

4.1.8 Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Eintrittsstellen sind Webseiten, gemeinsame Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs, Disketten usw.).

Wenn Ihr Computer Symptome einer Infektion mit Schadsoftware aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

- Starten Sie ESET Smart Security, und klicken Sie auf **Computer prüfen**
- Klicken Sie auf **Standardprüfung** (weitere Informationen vgl. Standardprüfung).
- Nachdem die Prüfung abgeschlossen ist, überprüfen Sie im Log die Anzahl der geprüften, infizierten und wiederhergestellten Dateien.

Wenn Sie nur einen Teil Ihrer Festplatte prüfen möchten, wählen Sie **Prüfen mit speziellen Einstellungen**, und wählen Sie die Bereiche aus, die auf Viren geprüft werden sollen.

Das folgende allgemeine Beispiel soll veranschaulichen, wie in ESET Smart Security mit Schadsoftware umgegangen wird. Nehmen wir einmal an, die Echtzeit-Systemüberwachung verwendet die Standard-Entfernungsstufe und erkennt eingedrungene Schadsoftware. Im Folgenden wird der Versuch gestartet, den Schadcode aus der Datei zu entfernen oder die Datei zu löschen. Ist für den Echtzeit-Schutz keine vordefinierte Aktion angegeben, müssen Sie in einem Warnungsfenster zwischen verschiedenen Optionen wählen. In der Regel stehen die Optionen **Schadcode entfernen**, **Löschen** und **Belassen** zur Auswahl. Es wird nicht empfohlen, die Option **Belassen** zu wählen, da sonst die infizierten Dateien nicht behandelt werden. Einzige Ausnahme: Sie sind sich sicher, dass die Datei harmlos ist und versehentlich erkannt wurde.

Schadcode entfernen und löschen
Entfernen Sie den Schadcode, wenn eine „saubere" Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

Wenn eine infizierte Datei „gesperrt" ist oder von einem Systemprozess verwendet wird, muss die Datei in der Regel erst freigegeben werden (häufig ist dazu ein Systemneustart erforderlich), bevor sie gelöscht werden kann.

Dateien in Archiven löschen
Im Standardmodus wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Mit anderen Worten: Im Standardmodus werden Archive nicht gelöscht, wenn sie zusätzlich nicht infizierte Dateien enthalten. Die Option „Immer versuchen, automatisch zu entfernen" sollten Sie allerdings mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und dies unabhängig vom Status der übrigen Archivdateien.

4.2 Personal Firewall

Die Personal Firewall kontrolliert den gesamten Netzwerkdatenverkehr vom und zum System. Dabei werden einzelne Netzwerkverbindungen anhand zuvor festgelegter Filterregeln zugelassen oder blockiert. Die Firewall bietet Schutz gegen Angriffe von Remotecomputern und ermöglicht die Blockierung bestimmter Dienste. Sie bietet außerdem Virenschutz für die Protokolle HTTP und POP3. Diese Funktionalität leistet einen äußerst wichtigen Beitrag zur Sicherheit Ihres Computers.

4.2.1 Filtermodus

Für die Personal Firewall von ESET Smart Security stehen fünf verschiedene Filtermodi zur Verfügung. Das Verhalten der Firewall hängt vom ausgewählten Modus ab. Die Filtermodi beeinflussen auch den Umfang der erforderlichen Benutzereingaben.

Folgende fünf Optionen stehen zur Verfügung:

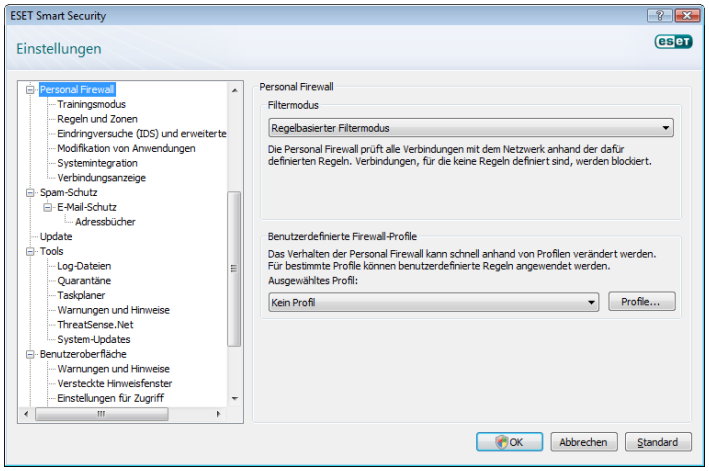
Automatischer Filtermodus – Standardmodus Dieser Modus ist für Benutzer geeignet, die eine einfache und komfortable Verwendung der Firewall bevorzugen, bei der keine Regeln definiert werden müssen. Im automatischen Filtermodus werden alle ausgehenden Verbindungen des entsprechenden Systems zugelassen und alle neuen Verbindungen blockiert, die von der Netzwerkseite ausgehen.

Automatischer Filtermodus mit Ausnahmen (benutzerdefinierte Regeln) – Entspricht dem automatischen Filtermodus, ermöglicht jedoch das Hinzufügen benutzerdefinierter Regeln.

Interaktiver Filtermodus – Ermöglicht die exakt auf Ihre Bedürfnisse zugeschnittene Konfiguration der Personal Firewall. Bei jeder Verbindung, für die keine Regel besteht, wird ein Dialogfenster mit einem Hinweis auf die unbekannte Verbindung angezeigt. Der Benutzer kann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll. Diese Auswahl kann als neue Regel für die Personal Firewall übernommen werden. Wird eine neue Regel erstellt, werden künftig alle Verbindungen dieser Art der Regel entsprechend zugelassen oder blockiert.

Regelbasierter Filtermodus – Blockierung aller Verbindungen, die nicht durch eine entsprechende Regel zugelassen werden. Mit diesem Modus können erfahrene Benutzer Regeln festlegen, um nur erwünschte und sichere Verbindungen zuzulassen. Alle anderen Verbindungen werden durch die Personal Firewall blockiert.

Trainingsmodus – Regeln werden automatisch erstellt und gespeichert. Dieser Modus ist für die anfängliche Konfiguration der Personal Firewall geeignet. Es ist keine Benutzerinteraktion erforderlich, da ESET Smart Security die Regeln entsprechend der vordefinierten Parameter speichert. Der Trainingsmodus ist nicht sicher und sollte nur verwendet werden, bis alle Regeln für die erforderlichen Verbindungen erstellt wurden.



4.2.2 Profile

Profile sind ein Hilfsmittel, um das Verhalten der Personal Firewall von ESET Smart Security zu steuern. Beim Erstellen oder Bearbeiten einer Regel der Personal Firewall können Sie diese Regel einem bestimmten Profil zuordnen oder auf alle Profile anwenden. Wenn Sie ein Profil auswählen, werden nur die globalen Regeln (ohne Angabe eines Profils) sowie die diesem Profil zugeordneten Regeln angewendet. Sie können mehrere Profile erstellen, denen unterschiedliche Regeln zugeordnet sind, um so auf einfache Weise das Verhalten der Personal Firewall anzupassen.

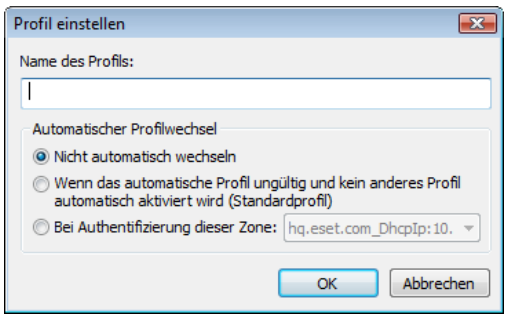
4.2.2.1 Profilverwaltung

Klicken Sie auf die Schaltfläche **„Profile..."** (siehe Abbildung in Abschnitt 4.2.1, „Filtermodus), um das Fenster mit den **Firewall-Profilen** zu öffnen, wo Sie Profile **hinzufügen**, **bearbeiten** und **entfernen** können. Beachten Sie, dass ein Profil zum **Bearbeiten** oder **Entfernen** nicht im Dropdown-Menü „Ausgewähltes Profil" ausgewählt sein darf. Beim Hinzufügen oder Bearbeiten eines Profils können Sie auch die Bedingungen definieren, unter denen das Profil aktiviert wird. Folgende Möglichkeiten stehen zur Verfügung:

Nicht automatisch wechseln – Die automatische Aktivierung ist ausgeschaltet (das Profil muss manuell aktiviert werden).

Wenn das automatische Profil ungültig und kein anderes Profil automatisch aktiviert wird (Standardprofil) – Wenn das automatische Profil ungültig wird (Computer ist mit einem nicht vertrauenswürdigen Netzwerk verbunden – siehe Abschnitt 4.2.6.1, „Netzwerkauthentifizierung") und kein anderes an dessen Stelle aktiviert wird (Computer ist mit keinem anderen vertrauenswürdigen Netzwerk verbunden), wechselt die Personal Firewall zu diesem Profil. Nur ein einziges Profil kann diese Aktivierung verwenden.

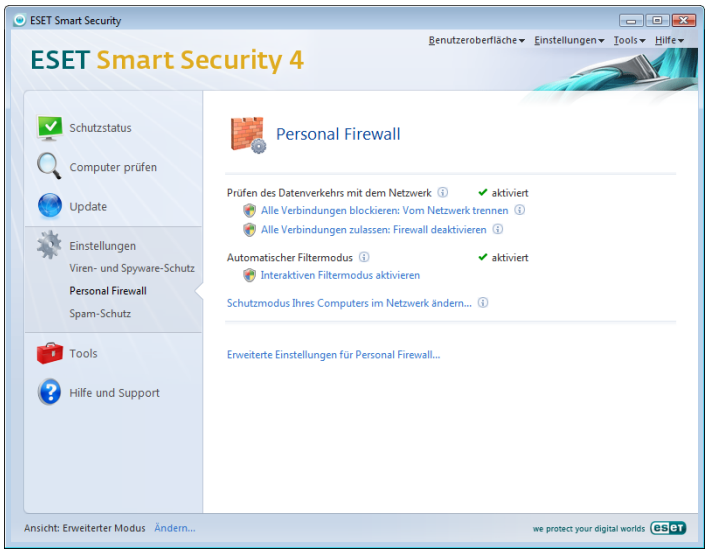
Bei Authentifizierung dieser Zone – Dieses Profil wird aktiviert, sobald die angegebene Zone authentifiziert ist (siehe Abschnitt 4.2.6.1, „Netzwerkauthentifizierung").



Wenn die Personal Firewall zu einem anderen Profil wechselt, wird in der rechten unteren Ecke neben der Systemuhr ein Hinweis angezeigt.

4.2.3 Alle Netzwerkverbindungen blockieren: Vom Netzwerk trennen

Für die vollständige Blockierung aller Netzwerkverbindungen existiert nur die Option **„Alle Verbindungen blockieren: Vom Netzwerk trennen“** Der gesamte eingehende und ausgehende Datenverkehr wird durch die Personal Firewall blockiert. Dabei wird keine Warnung angezeigt. Verwenden Sie diese Option nur, wenn Sie schwerwiegende Sicherheitsrisiken befürchten, die eine Trennung der Netzwerkverbindung erfordern.



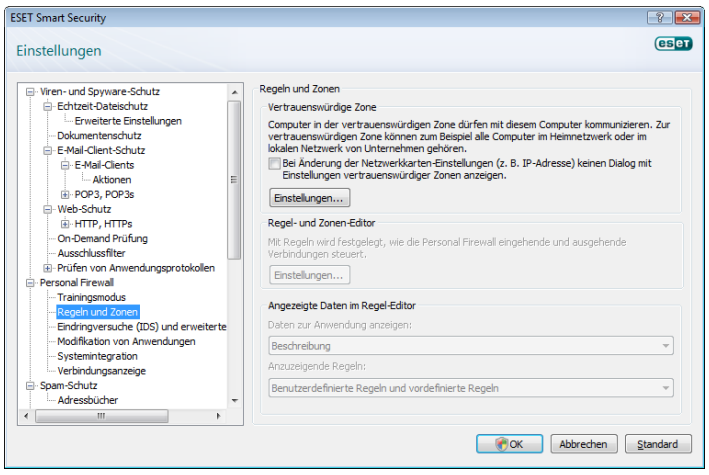
4.2.4 Filter deaktivieren: Firewall deaktivieren

Die Option „Filter deaktivieren“ bewirkt das Gegenteil der Option, den gesamten Netzwerkdatenverkehr zu blockieren. Wenn Sie diese Option auswählen, werden alle Filteroptionen der Personal Firewall deaktiviert und alle eingehenden und ausgehenden Verbindungen zugelassen. Das System verhält sich dann so, als wäre keine Firewall vorhanden.

4.2.5 Regeln konfigurieren und verwenden

Regeln fassen eine Reihe von Bedingungen zusammen, anhand derer alle Netzwerkverbindungen und mit diesen Bedingungen verknüpften Aktionen wirksam geprüft werden. In der Personal Firewall können Sie festlegen, welche Aktion erfolgen soll, wenn eine Verbindung aufgebaut wird, für die eine Regel besteht.

Um auf die Filtereinstellungen für Regeln zuzugreifen, klicken Sie auf **„Erweiterte Einstellungen** (F5) > **Personal Firewall** > **Regeln und Zonen“**. Um die aktuellen Einstellungen anzuzeigen, klicken Sie im Abschnitt **„Regel- und Zonen-Editor“** auf **„Einstellungen...“** (wenn der **automatische** Filtermodus für die Personal Firewall aktiviert ist, sind diese Einstellungen nicht verfügbar).



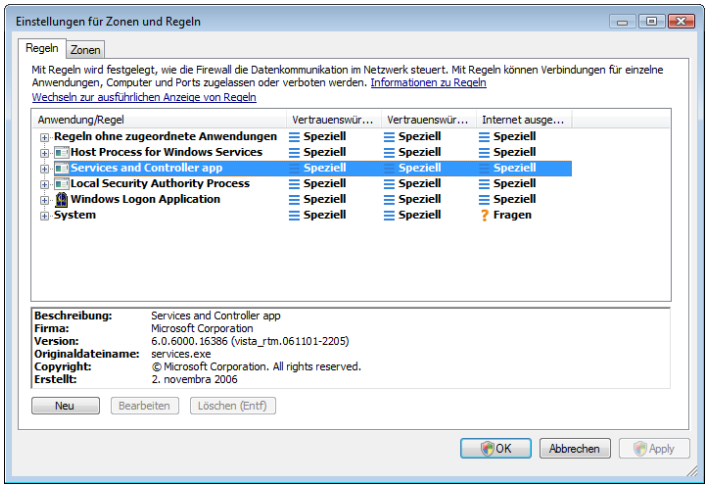
Im Fenster **„Einstellungen für Zonen und Regeln“** wird ein Überblick der Regeln oder Zonen angezeigt (je nach ausgewählter Registerkarte). Das Fenster ist in zwei Abschnitte unterteilt. Im oberen Abschnitt sind alle Regeln in einer Kurzansicht aufgeführt. Im unteren Abschnitt werden Details zur im oberen Abschnitt ausgewählten Regel angezeigt. Am unteren Fensterrand befinden sich die Schaltflächen **„Neu“**, **„Bearbeiten“** und **„Löschen (Entf)“**, über die Sie die Regeln konfigurieren können.

Die Verbindungen können in eingehende und ausgehende Verbindungen unterteilt werden. Eingehende Verbindungen gehen von einem Remotecomputer aus, der versucht, eine Verbindung zum lokalen System herzustellen. Ausgehende Verbindungen funktionieren in entgegengesetzter Richtung – die lokale Seite kontaktiert einen Remotecomputer.

Wenn eine neue, unbekannte Verbindung erkannt wird, sollten Sie genau prüfen, ob diese zugelassen oder blockiert werden soll. Unerwünschte, unsichere oder unbekannte Verbindungen können ein Sicherheitsrisiko für Ihren Computer darstellen. Wenn eine solche Verbindung aufgebaut wird, sollten Sie besonders auf die Gegenstelle achten und prüfen, welche Anwendung versucht, mit Ihrem Computer zu kommunizieren. Viele Schadprogramme versuchen, persönliche Daten zu erfassen, zu versenden oder weitere schädliche Anwendungen auf den Host-Computer zu laden. Mithilfe der Personal Firewall können Sie solche Verbindungen erkennen und beenden.

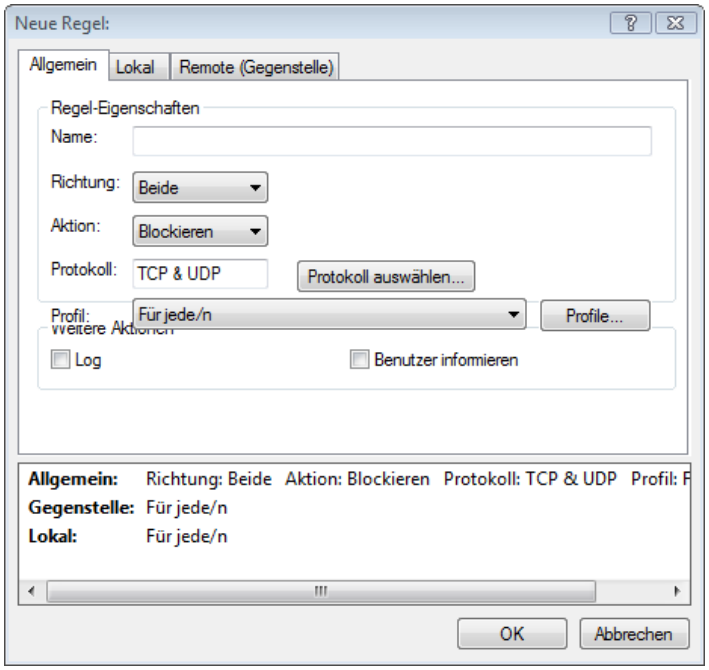
4.2.5.1 Neue Regel hinzufügen

Wenn eine neue Anwendung installiert wird, die auf das Netzwerk zugreift, oder wenn eine Veränderung an einer bestehenden Verbindung (Gegenstelle, Portnummer usw.) aufgetreten ist, muss eine neue Regel erstellt werden.



Um eine neue Regel zu erstellen, muss die Registerkarte **„Regeln“** ausgewählt sein. Klicken Sie im Fenster **„Einstellungen für Zonen und Regeln“** auf **„Neu“**. Durch Klicken auf diese Schaltfläche wird ein Dialogfenster geöffnet, in dem Sie eine neue Regel angeben können. Im oberen Teil des Fensters werden drei Registerkarten angezeigt:

- **Allgemein**: Geben Sie einen Regelnamen sowie die Verbindungsrichtung, die Aktion, das Protokoll und das Profil an, für das die Regel gelten soll.
- **Remote**: Auf dieser Registerkarte werden Informationen zum Remoteport (Portbereich) angezeigt. Außerdem können Sie hier eine Liste mit Remote-IP-Adressen oder Zonen für eine Regel angeben.
- **Lokal**: Es werden Informationen zur lokalen Seite der Verbindung angezeigt, z. B. die Nummer des lokalen Ports oder Portbereichs sowie der Name der kommunizierenden Anwendung.



Ein gutes Beispiel für eine neue Regel ist der Zugriff eines Webbrowsers auf das Netzwerk. Dazu müssen Sie Folgendes angeben:

- Aktivieren Sie auf der Registerkarte **„Allgemein“** ausgehende Verbindungen über TCP und UDP
- Geben Sie auf der Registerkarte **„Lokal“** den Prozess an, der Ihrer Browseranwendung entspricht (z. B. iexplore.exe für Internet Explorer)
- Aktivieren Sie auf der Registerkarte **„Remote“** Portnummer 80 nur, wenn Sie Standard-Internetdienste zulassen möchten.

4.2.5.2 Regeln bearbeiten

Um eine bestehende Regel zu bearbeiten, klicken Sie auf die Schaltfläche **„Bearbeiten“**. Alle Parameter (siehe hierzu Abschnitt 4.2.5.1, „Neue Regel erstellen“) können angepasst werden.

Eine Änderung der Einstellungen ist immer dann erforderlich, wenn sich die überwachten Parameter geändert haben. In diesem Fall erfüllt die Regel nicht die Bedingungen, und die angegebene Aktion kann nicht durchgeführt werden. Die entsprechende Verbindung wird eventuell blockiert, wodurch Probleme bei der Ausführung der jeweiligen Anwendung entstehen können. Ein typisches Beispiel hierfür ist eine Änderung der Netzwerkadresse oder Portnummer der Gegenstelle.

4.2.6 Zonen konfigurieren

Sie können im Fenster **„Einstellungen für Zonen“** den Zonennamen, die Beschreibung, die Liste der Netzwerkadressen und die Zonenauthentifizierung angeben (siehe Abschnitt 4.2.6.1.1, „Zonenauthentifizierung – Client-Konfiguration“).

Zonen sind eine Reihe von Netzwerkadressen, die eine logische Gruppe bilden. Jeder Adresse in einer Gruppe werden ähnliche Regeln zugewiesen, die zentral für die Gruppe festgelegt werden können. Ein Beispiel für eine solche Gruppe ist die vertrauenswürdige Zone. Die vertrauenswürdige Zone ist eine Gruppe von Netzwerkadressen, die als vertrauenswürdig eingestuft und durch die Personal Firewall in keiner Weise blockiert werden.

Diese Zonen können durch Klicken auf die Schaltfläche **„Neu“** auf der Registerkarte **„Zonen“** im **Einstellungsfenster für Zonen und Regeln** konfiguriert werden. Geben Sie einen **Namen** und eine **Beschreibung** für die Zone ein, und fügen Sie eine Remote-IP-Adresse hinzu, indem Sie auf die Schaltfläche **„IPv4-Adresse hinzufügen“** klicken.

4.2.6.1 Netzwerkauthentifizierung

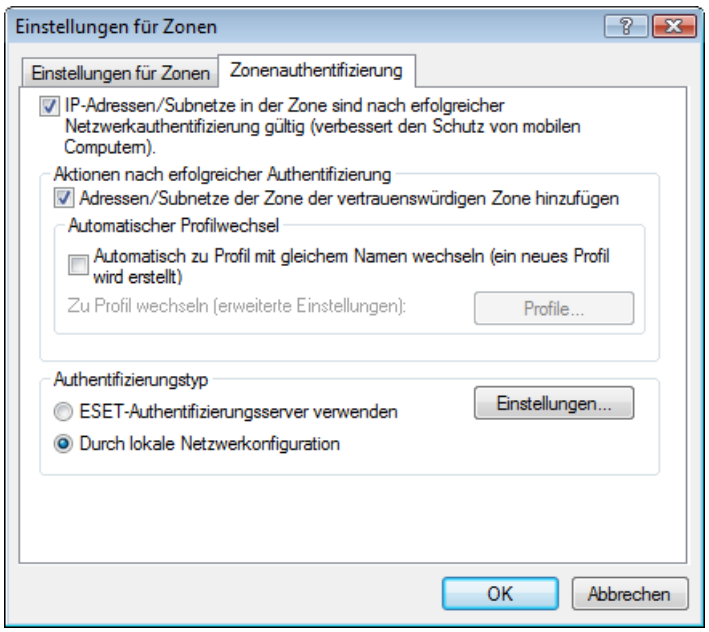
Die vertrauenswürdige Zone wird durch die lokale IP-Adresse der Netzwerkkarte identifiziert. Mobile Computer melden sich oft an Netzwerken mit IP-Adressen an, die jenen der vertrauenswürdigen Netzwerke gleichen. Werden die Einstellungen für die vertrauenswürdige Zone nicht manuell auf **„Maximaler Schutz“** gesetzt, verwendet die Personal Firewall weiterhin den Modus **„Zugriff zulassen“**.

Um solche Situationen zu vermeiden, sucht die Zonenauthentifizierung nach einem bestimmten Server im Netzwerk und verwendet zur Serverauthentifizierung eine asymmetrische Verschlüsselung (RSA). Die Authentifizierung wird für jedes Netzwerk wiederholt, mit dem sich der Computer verbindet.

4.2.6.1.1 Zonenauthentifizierung – Client-Konfiguration

Klicken Sie im **Einstellungsfenster für Zonen und Regeln** auf die Registerkarte **„Zonen“**, und erstellen Sie eine neue Zone. Verwenden Sie dabei den Namen der durch den Server authentifizierten Zone. Klicken Sie anschließend auf **„IPv4-Adresse hinzufügen“**, und wählen Sie die Option **„Subnetz“** aus, um eine Subnetzmaske hinzuzufügen, die den Authentifizierungsserver enthält.

Klicken Sie auf die Registerkarte **„Zonenauthentifizierung“**, und wählen Sie die Option **„IP-Adressen/Subnetze in der Zone sind nach erfolgreicher Authentifizierung des Servers im Netzwerk gültig“**. Ist diese Option ausgewählt, wird die Zone bei nicht erfolgreicher Authentifizierung ungültig. Klicken Sie auf **„Profile...“**, um ein Personal Firewall-Profil auszuwählen, das nach erfolgreicher Zonenauthentifizierung aktiviert werden soll. Wenn Sie die Option **„Adressen/Subnetze der Zone der vertrauenswürdigen Zone hinzufügen“** auswählen, werden die Adressen/Subnetze der Zone nach erfolgreicher Authentifizierung zur vertrauenswürdigen Zone hinzugefügt (empfohlen).



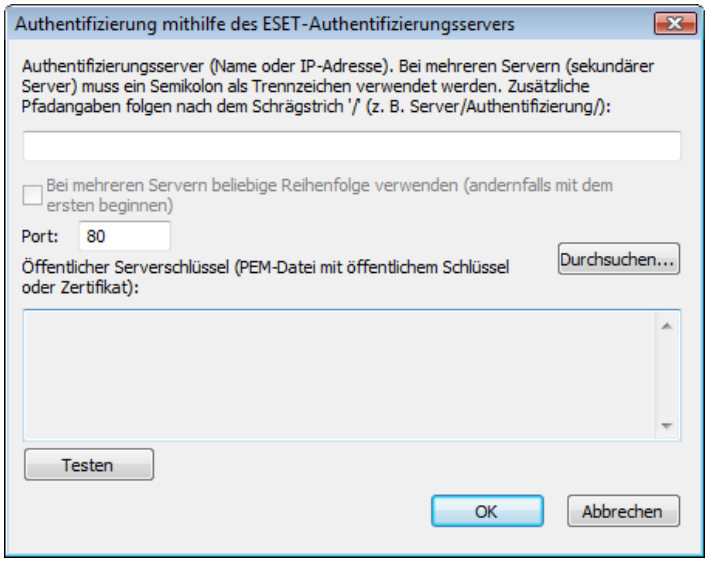
Es sind drei Authentifizierungstypen verfügbar:

1) ESET-Authentifizierungsserver verwenden

Klicken Sie auf **„Einstellungen...“**, und geben Sie einen Servernamen, einen Listening-Port für den Server und einen öffentlichen Serverschlüssel an, der dem privaten Serverschlüssel entspricht (siehe Abschnitt 4.2.6.1.2, „Zonenauthentifizierung – Server-Konfiguration“). Der Servername kann in Form einer IP-Adresse, eines DNS- oder NetBios-Namens angegeben werden. Der Servername kann von einem Pfad gefolgt sein, der den Speicherort des Schlüssels auf dem Server angibt (z. B. Server_Name_/Verzeichnis1/Verzeichnis2/Authentifizierung). Geben Sie mehrere Server an (jeweils voneinander durch Semikolon getrennt), die als alternative Server agieren, falls der erste nicht verfügbar ist.

Der öffentliche Schlüssel kann einer der folgenden Dateitypen sein:

- PEM-verschlüsselter öffentlicher Schlüssel (.pem) – dieser Schlüssel kann mithilfe des ESET-Authentifizierungsservers generiert werden (siehe Abschnitt 4.2.6.1.2, „Zonenauthentifizierung – Server-Konfiguration“).
- Codierter öffentlicher Schlüssel
- Zertifikat für öffentlichen Schlüssel (.crt)


Authentifizierung mithilfe des ESET-Authentifizierungsservers
Authentifizierungsserver (Name oder IP-Adresse). Bei mehreren Servern (sekundärer Server) muss ein Semikolon als Trennzeichen verwendet werden. Zusätzliche Pfadangaben folgen nach dem Schrägstrich '/' (z. B. Server/Authentifizierung/):
Bei mehreren Servern beliebige Reihenfolge verwenden (andernfalls mit dem ersten beginnen)
Port: 80
Öffentlicher Serverschlüssel (PEM-Datei mit öffentlichem Schlüssel oder Zertifikat):
Durchsuchen...
Testen
OK
Abbrechen

Um die Einstellungen zu testen, klicken Sie auf **„Testen“**. Ist die Authentifizierung erfolgreich, wird die Meldung *Serverauthentifizierung erfolgreich* angezeigt. Wenn die Authentifizierung nicht korrekt konfiguriert ist, wird eine der folgenden Fehlermeldungen angezeigt:

Fehler bei der Serverauthentifizierung. Die maximale Authentifizierungszeit ist abgelaufen.
Auf den Authentifizierungsserver kann nicht zugegriffen werden. Überprüfen Sie den Servernamen/die IP-Adresse, und/oder prüfen Sie die Einstellungen der Personal Firewall für die Bereiche Client und Server.

Fehler bei der Kommunikation mit dem Server.
Der Authentifizierungsserver wird nicht ausgeführt. Starten Sie den Authentifizierungsserver-Dienst (siehe Abschnitt 4.2.6.1.2, „Zonenauthentifizierung – Server-Konfiguration“).

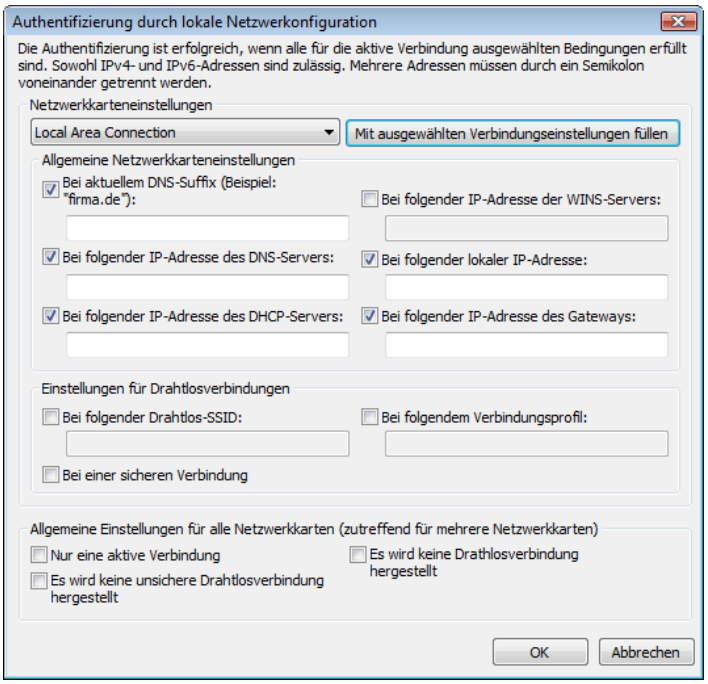
Der Name der Authentifizierungszone und die Serverzone stimmen nicht überein.
Der konfigurierte Zonenname entspricht nicht der Zone des Authentifizierungsservers. Überprüfen Sie beide Zonen, und stellen Sie sicher, dass ihre Namen identisch sind.

Fehler bei der Serverauthentifizierung. Serveradresse konnte in der Adressliste der angegebenen Zone nicht gefunden werden.
Die IP-Adresse des Computers, auf dem der Authentifizierungsserver ausgeführt wird, befindet sich außerhalb des in der aktuellen Zonenkonfiguration definierten IP-Adressbereichs.

Fehler bei der Serverauthentifizierung. Es wurde möglicherweise ein ungültiger öffentlicher Schlüssel eingegeben.
Überprüfen Sie, ob der angegebene öffentliche Schlüssel dem privaten Serverschlüssel entspricht. Überprüfen Sie auch, ob die Datei des öffentlichen Schlüssels beschädigt ist.

2) Durch lokale Netzwerkkonfiguration

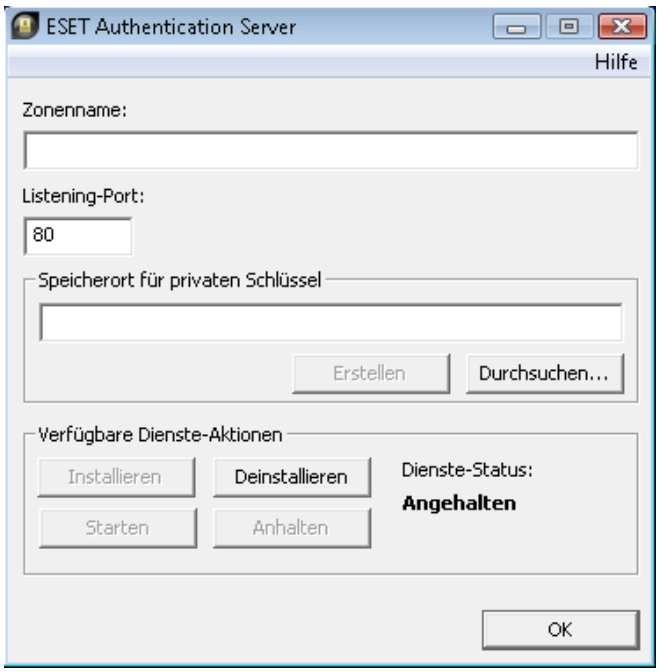
Die Authentifizierung erfolgt entsprechend den Parametern einer lokalen Netzwerkkarte. Die Authentifizierung ist erfolgreich, wenn alle ausgewählten Parameter für die aktive Verbindung gültig sind.


Authentifizierung durch lokale Netzwerkkonfiguration
Die Authentifizierung ist erfolgreich, wenn alle für die aktive Verbindung ausgewählten Bedingungen erfüllt sind. Sowohl IPv4- und IPv6-Adressen sind zulässig. Mehrere Adressen müssen durch ein Semikolon voneinander getrennt werden.
Netzwerkkarteneinstellungen
Local Area Connection
Mit ausgewählten Verbindungseinstellungen füllen
Allgemeine Netzwerkkarteneinstellungen
Bei aktuellem DNS-Suffix (Beispiel: "firma.de"):
Bei folgender IP-Adresse der WINS-Servers:
Bei folgender IP-Adresse des DNS-Servers:
Bei folgender lokaler IP-Adresse:
Bei folgender IP-Adresse des DHCP-Servers:
Bei folgender IP-Adresse des Gateways:
Einstellungen für Drahtlosverbindungen
Bei folgender Drahtlos-SSID:
Bei folgendem Verbindungsprofil:
Bei einer sicheren Verbindung
Allgemeine Einstellungen für alle Netzwerkkarten (zutreffend für mehrere Netzwerkkarten)
Nur eine aktive Verbindung
Es wird keine Drahtlosverbindung hergestellt
Es wird keine unsichere Drahtlosverbindung hergestellt
OK
Abbrechen

4.2.6.1.2 Zonenauthentifizierung – Server-Konfiguration

Die Authentifizierung kann durch jeden Computer/Server ausgeführt werden, der mit dem zu authentifizierenden Netzwerk verbunden ist. Die Anwendung für den ESET-Authentifizierungsserver muss auf einem Computer/Server installiert sein, der jederzeit für die Authentifizierung verfügbar ist, wenn ein Client versucht, eine Verbindung zum Netzwerk herzustellen. Die Installationsdatei der Anwendung für den ESET-Authentifizierungsserver kann von der Website von ESET heruntergeladen werden.

Nach der Installation der Anwendung für den ESET-Authentifizierungsserver wird ein Dialogfenster angezeigt (Sie können unter **„Start > Alle Programme > ESET > ESET Auth Server > ESET Auth Server“** jederzeit auf die Anwendung zugreifen).



Zum Konfigurieren des Authentifizierungsservers geben Sie den Namen der Authentifizierungszone, den Listening-Port für den Server (standardmäßig Port 80) sowie den Speicherort für das öffentliche und das private Schlüsselpaar ein. Erstellen Sie anschließend den öffentlichen und den privaten Schlüssel, die bei der Authentifizierung verwendet werden. Der private Schlüssel verbleibt auf dem Server, während der öffentliche Schlüssel clientseitig im Abschnitt „Zonenauthentifizierung“ beim Einrichten einer Zone in den Einstellungen der Firewall importiert werden muss.

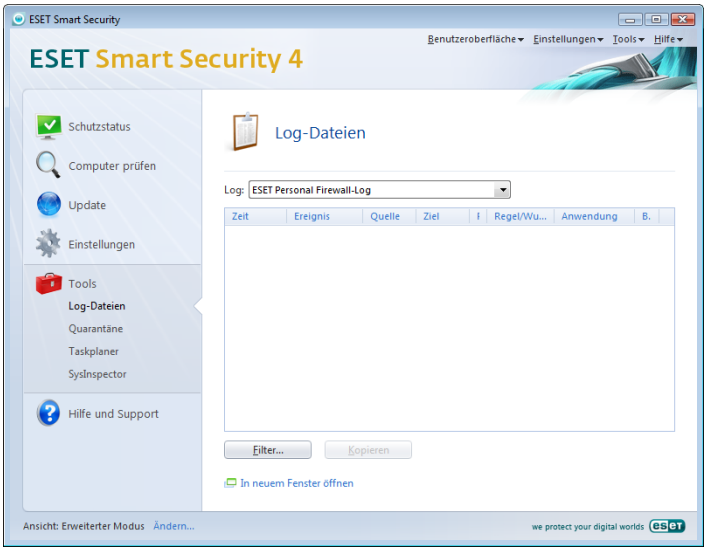
4.2.7 Verbindung herstellen – Erkennung

Die Personal Firewall erkennt jede neu erstellte Netzwerkverbindung. Durch den aktivierten Firewall-Modus wird bestimmt, welche Vorgänge für die neue Regel ausgeführt werden. Bei aktiviertem automatischen oder regelbasierten Filtermodus führt die Firewall die vordefinierten Vorgänge automatisch und ohne Eingriffe des Benutzers aus. Im interaktiven Filtermodus wird bei einer neu erkannten Netzwerkverbindung ein Fenster mit genauen Informationen zur Verbindung angezeigt. Sie können dann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll. Wenn Sie wiederholt dieselbe Verbindung im Dialogfenster zulassen, sollten Sie eine neue Regel für diese Verbindung erstellen. Wählen Sie dazu die Option **„Auswahl dauerhaft anwenden (Regel erstellen)“**. Speichern Sie den Vorgang als neue Regel für die Personal Firewall. Wenn die Firewall dieselbe Verbindung später erkennt, wird die entsprechende Regel angewendet.

ESET Smart Security 4
Eingehende Verbindung
Vertrauenswürdige Zone
Ein Remote Computer aus einer vertrauenswürdigen Zone versucht, eine Verbindung zu einer Anwendung auf diesem Computer herzustellen. Kommunikation zulassen?
Anwendung: Host Process for Windows Services
Herausgeber: Microsoft Windows
Remote Computer: ADMIN-PC (10.1.109.126)
Lokaler Port: 5355 (llmnr)
Auswahl dauerhaft anwenden (Regel erstellen)
Aktion für Prozess vorübergehend anwenden
Zulassen
Blockieren
Erweiterte Einstellungen anzeigen

Gehen Sie beim Erstellen neuer Regeln vorsichtig vor. Lassen Sie nur sichere Verbindungen zu. Werden alle Verbindungen zugelassen, kann die Firewall ihre Aufgabe nicht erfüllen. Beachten Sie die folgenden wichtigen Parameter für Verbindungen:

- **Gegenstelle:** Lassen Sie nur Verbindungen mit vertrauenswürdigen und bekannten Adressen zu
- **Lokale Anwendung:** Es wird davon abgeraten, Verbindungen für unbekannte Anwendungen oder Prozesse zuzulassen
- **Portnummer:** Verbindungen über übliche Ports (z. B. Web – Portnummer 80) sollten im Regelfall zugelassen werden



Schadsoftware wird häufig über das Internet oder über versteckte Verbindungen verbreitet, um fremde Systeme zu infizieren. Wenn die Regeln richtig eingestellt werden, ist die Personal Firewall ein wirksames Hilfsmittel zum Schutz vor verschiedensten Schadcode-Angriffen.

4.2.8 Erstellen von Logs

Die Personal Firewall von ESET Smart Security speichert alle wichtigen Ereignisse in einer Log-Datei, die direkt vom Hauptmenü aus aufgerufen werden kann. Klicken Sie auf **„Tools > Log-Dateien“**. Wählen Sie dann im Dropdown-Menü **„Log“** die Option **„ESET Personal Firewall-Log“**.

Die Log-Dateien sind ein wertvolles Hilfsmittel zur Fehlererkennung sowie zur Entdeckung von eingedrungenem Schadcode und sollten daher entsprechend genutzt werden. Die Log-Dateien der ESET Personal Firewall enthalten folgende Informationen:

- Datum und Uhrzeit des Ereignisses
- Bezeichnung des Ereignisses
- Ursprungsadresse
- Zieladresse
- Übertragungsprotokoll
- Zugewiesene Regel oder, falls identifiziert, Name des Wurms
- Beteiligte Anwendung
- Benutzer

Eine gründliche Analyse dieser Daten kann wesentlich dazu beitragen, Angriffe auf die Systemsicherheit zu erkennen. Viele andere Faktoren können auf Sicherheitsrisiken hinweisen und geben Ihnen die Möglichkeit, mögliche Auswirkungen zu minimieren: überdurchschnittlich häufige Verbindungen von unbekannten Standorten, ungewöhnlich viele Verbindungsversuche, Verbindungen mit unbekannten Anwendungen, Verwendung ungewöhnlicher Portnummern.

4.3 Spam-Schutz

Spam, d. h. der Empfang unerwünschter E-Mail-Nachrichten, ist ein zentrales Problem der elektronischen Kommunikation. Spam macht bis zu 80 Prozent der gesamten E-Mail-Kommunikation aus. Der Spam-Schutz nimmt dieses Problem in Angriff. Verschiedene äußerst effiziente Verfahren sorgen für ausgezeichnete Filterquoten.

Ein zentrales Prinzip beim Spam-Schutz ist die Möglichkeit der Erkennung unerwünschter E-Mails über eine Whitelist bzw. Blacklist. In der Whitelist werden vertrauenswürdige E-Mail-Adressen, in der Blacklist Spam-Adressen vorab definiert. Alle Adressen Ihres E-Mail-Programms sowie alle vom Benutzer als „sicher" eingestuften Adressen werden automatisch der Whitelist hinzugefügt.

Die primäre Methode zur Spam-Erkennung ist die Prüfung der E-Mail-Eigenschaften. Empfangene Nachrichten werden anhand grundlegender Spam-Kriterien und mithilfe spezifischer Methoden (Nachrichtendefinitionen, statistische Heuristik, Erkennung von Algorithmen usw.) geprüft. Der sich daraus ergebende Indexwert entscheidet darüber, ob eine Nachricht als Spam eingestuft wird oder nicht.

Auch der bayessche Filter wird eingesetzt. Mit der Einstufung einer Nachricht als *Spam* oder *Kein Spam* legt der Benutzer gleichzeitig eine Datenbank mit den Wörtern an, die in der jeweiligen Nachrichten-Kategorie vorkommen. Je größer die Datenbank, desto genauer die Ergebnisse.

Werden die oben erwähnten Methoden miteinander kombiniert, steigt die Spam-Erkennungsrate.

ESET Smart Security unterstützt Spam-Schutz für Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail und Mozilla Thunderbird.

4.3.1 Intelligenter Spam-Schutz

Der intelligente Spam-Schutz bedient sich des oben genannten bayesschen Filters. Die Relevanz einzelner Wörter wird im Verlauf des Einstufungsprozesses der einzelnen Nachrichten (Spam/Kein Spam) fortlaufend neu bewertet. Je mehr Nachrichten eingestuft werden, desto genauer sind die mit dem bayesschen Filter erzielten Resultate.

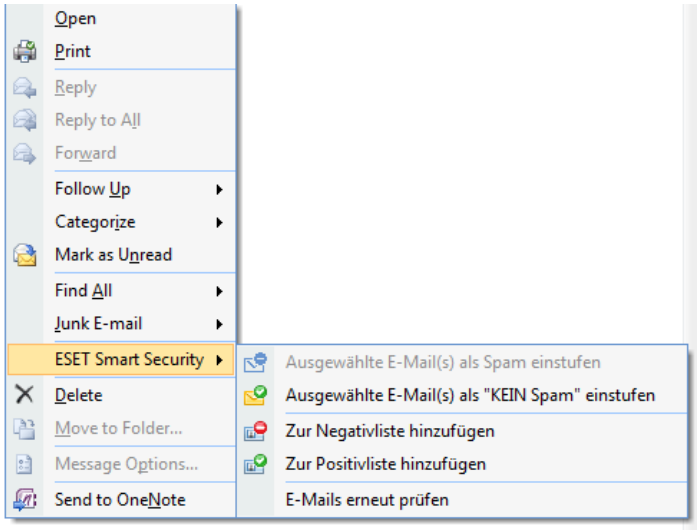
Fügen Sie der Whitelist bekannte Adressen hinzu, um E-Mails mit diesem Absender von der Filterung auszunehmen.

4.3.1.1 Adressen zur Whitelist hinzufügen

E-Mail-Adressen von Personen, mit denen der Benutzer häufig kommuniziert, können in die Liste „sicherer" Adressen, die sog. Whitelist, aufgenommen werden. Auf diese Weise wird sichergestellt, dass keine Nachricht, die von einer Adresse aus der Whitelist stammt, als Spam eingestuft wird. Um der Whitelist eine neue Adresse hinzuzufügen, klicken Sie mit der rechten Maustaste auf die entsprechende E-Mail-Nachricht, und wählen Sie im Kontextmenü unter „ESET Smart Security" **Zur Whitelist hinzufügen**. Alternativ können Sie oben in Ihrem E-Mail-Programm in der ESET-Symbolleiste die Option **Vertrauenswürdige Adresse** wählen.
Bei Spam-Adressen können Sie genauso vorgehen. Jede E-Mail von einer in der Blacklist aufgeführten E-Mail-Adresse wird als Spam eingestuft.

4.3.1.2 E-Mails als Spam einstufen

Jede im E-Mail-Programm angezeigte Nachricht kann als Spam eingestuft werden. Verwenden Sie dazu entweder das Kontextmenü (Klick mit der rechten Maustaste > **ESET Smart Security > Ausgewählte E-Mails als Spam einstufen**), oder klicken Sie in der Spam-Schutz-Symbolleiste von ESET Smart Security in Ihrem E-Mail-Programm auf **Spam**.



Als Spam eingestufte Nachrichten werden automatisch in den SPAM-Ordner verschoben. Die E-Mail-Adresse des Absenders wird jedoch nicht automatisch in die Blacklist aufgenommen. Gleichermaßen können Sie Nachrichten als „KEIN Spam" einstufen. Nachrichten aus dem Ordner **Spam-E-Mails** werden in den ursprünglichen Ordner verschoben, wenn sie als „Kein Spam" klassifiziert werden. Die E-Mail-Adresse des Absenders wird nicht automatisch in die Whitelist aufgenommen.

4.4 Programm aktualisieren

Eine regelmäßige Aktualisierung des Programms ist die grundlegende Voraussetzung dafür, dass ESET Smart Security den größtmöglichen Schutz bieten kann. Mit dem Update-Modul wird gewährleistet, dass das Programm stets auf dem neuesten Stand ist. Dabei werden zwei Methoden kombiniert–die Aktualisierung der Signaturdatenbank und die Aktualisierung der Systemkomponenten.

Informationen über den aktuellen Update - Status finden Sie unter der Option **Update**. Dort werden Informationen zur aktuellen Version der Signaturdatenbank angezeigt, und Sie sehen, ob eine Aktualisierung erforderlich ist. Darüber hinaus kann an dieser Stelle auch der Update -Vorgang sofort gestartet werden. Nutzen Sie dazu die Option – **Update der Signaturdatenbank** – Außerdem können Sie grundlegende Einstellungen für Updates vornehmen, z. B. den Benutzernamen und das Passwort für die Update - Server von ESET eintragen.

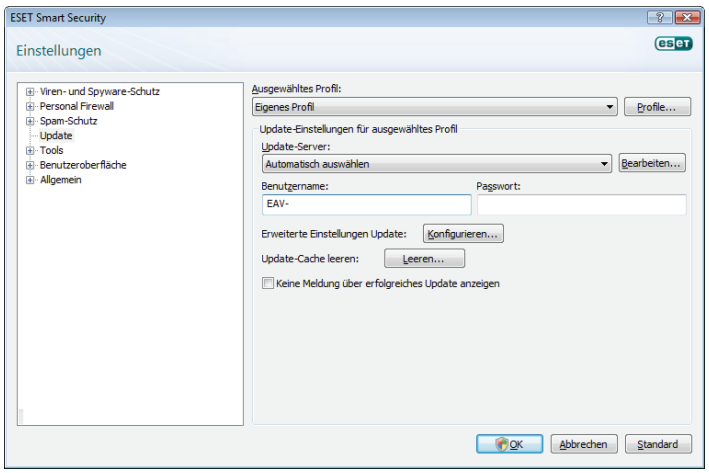
Im Informationsfenster werden weitere Details wie das Datum und die Uhrzeit des letzten erfolgreichen Updates und die Nummer der Signaturdatenbank angezeigt. Diese Nummer ist ein aktiver Link zur Website von ESET, auf der alle Signaturen aufgeführt werden, die bei dem entsprechenden Update hinzugefügt wurden.

Verwenden Sie den Link **Registrieren**, um das Registrierungsformular zu öffnen, über das erreicht wird, dass Ihre neue Lizenz bei ESET registriert wird und Ihre Authentifizierungsdaten anschließend an Ihre E-Mail-Adresse gesendet werden.

HINWEIS: Sie erhalten den Benutzernamen und das Passwort von ESET nach dem Kauf von ESET Smart Security.

4.4.1 Update-Einstellungen

In den Einstellungen für Updates finden Sie Informationen zum Ursprung von Updates, z. B. die Liste der Update-Server und die Authentifizierungsdaten für diese Server. Standardmäßig ist für das Feld **Update-Server:** die Einstellung **Automatisch auswählen** festgelegt. Mit dieser Option wird gewährleistet, dass Update-Dateien automatisch von den ESET-Update-Servern heruntergeladen werden und gleichzeitig der Netzwerk-Datenverkehr der einzelnen Update-Server berücksichtigt wird. Die Einstellungen für Updates finden Sie in den erweiterten Einstellungen (F5) unter **Update**.



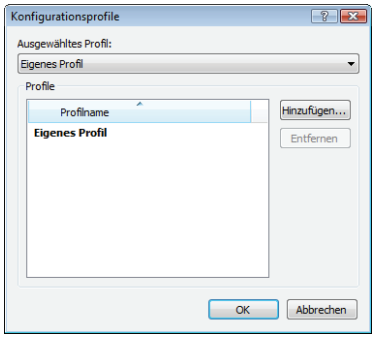
Die Liste der aktuellen Update-Server kann im **Update-Server:** Dropdown-Menü aus. Um einen neuen Update-Server hinzuzufügen, klicken Sie im Bereich **Update-Einstellungen für ausgewähltes Profil** auf **Bearbeiten...**. Klicken Sie anschließend auf **Hinzufügen**.

Zur Authentifizierung müssen der **Benutzername** und das **Passwort** eingeben werden, die Sie nach dem Kauf der ESET-Produktlizenz erhalten haben.

4.4.1.1 Update-Profile

Für verschiedene Update-Konfigurationen können benutzerdefinierte Update-Profile erstellt werden, die für bestimmte Update-Tasks verwendet werden. Besonders sinnvoll ist das Erstellen verschiedener Update-Profile für mobile Benutzer, bei denen sich bei der Internetverbindung häufig Änderungen ergeben. Mobile Benutzer können den Update-Task so ändern, dass anstelle der unter **Mein Profil** angegebenen Konfiguration ein alternatives Profil verwendet wird, wenn ein Update mit dem ersten Profil nicht möglich ist.

Im Dropdown-Menü **Ausgewähltes Profil** wird das gegenwärtig verwendete Profil angezeigt. Standardmäßig ist dies **Mein Profil**. Zum Erstellen eines neuen Profils klicken Sie auf **Profile...** und dann auf **Hinzufügen...**. Geben Sie anschließend den **Namen des Profils** ein. Beim Erstellen eines neuen Profils können Sie über **Einstellungen kopieren von Profil:** die Einstellungen eines vorhandenen Profils übernehmen.



In den Profileinstellungen können Sie den Update-Server angeben, zu dem das Programm eine Verbindung für den Download von Updates herstellt. Dies kann ein beliebiger Server aus der Liste der verfügbaren Server oder ein neu hinzugefügter Server sein. Die Liste der aktuellen Update-Server kann im **Update-Server:** Dropdown-Menü abgerufen werden. Um einen neuen Update-Server hinzuzufügen, klicken Sie im Bereich **Update-Einstellungen für ausgewähltes Profil** auf **Bearbeiten...**. Klicken Sie anschließend auf **Hinzufügen**.

4.4.1.2 Erweiterte Einstellungen für Updates

Um **Erweiterte Einstellungen Update** anzuzeigen, klicken Sie auf **Einstellungen...**. Zu den erweiterten Einstellungen gehören Optionen für **Update-Modus, HTTP-Proxy, LAN** und **Update-Mirror**.

4.4.1.2.1 Update-Modus

Auf der Registerkarte **Update-Modus** finden Sie Optionen zum Aktualisieren der Programmkomponenten.

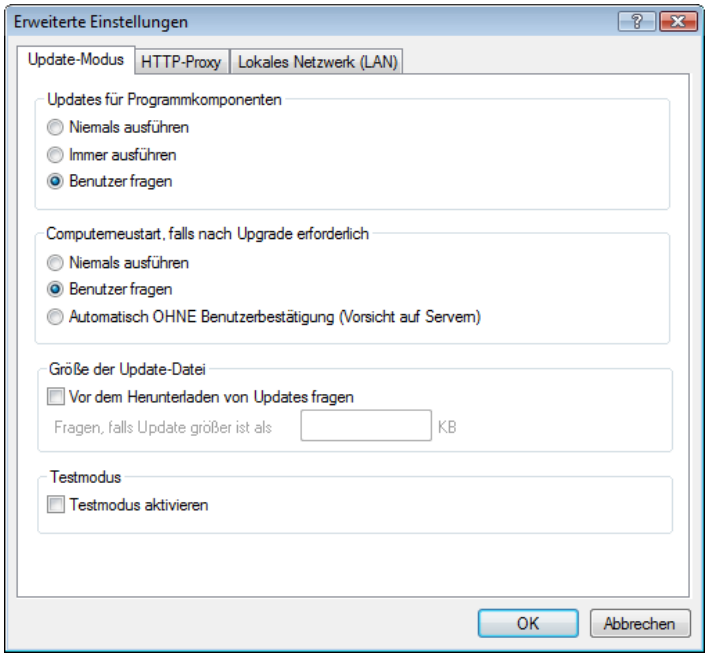
Im Abschnitt **Updates für Programmkomponenten** stehen drei Optionen zur Verfügung:

- **Programmkomponenten nicht aktualisieren**
- **Immer ausführen**
- **Benutzer fragen**

Wenn Sie die Option **Programmkomponenten nicht aktualisieren** wählen, werden neue Updates für Programmkomponenten, die von ESET veröffentlicht wurden, nicht heruntergeladen, und auf dem entsprechenden Computer erfolgt keine Aktualisierung von Programmkomponenten. Wenn Sie die Option **Programmkomponenten automatisch aktualisieren** wählen, werden Updates für Programmkomponenten immer ausgeführt, sobald ein neues Update auf den ESET-Update-Servern verfügbar ist, und die entsprechende Programmkomponente wird durch das Herunterladen der neuen Version aktualisiert.

Wählen Sie die dritte Option, **Benutzer fragen**, wenn Sie das Herunterladen neu verfügbarer Updates zuvor durch den Benutzer bestätigen lassen möchten. In diesem Fall wird ein Dialogfenster mit Informationen zum verfügbaren Update angezeigt, und der Benutzer kann entscheiden, ob das Update bestätigt oder abgelehnt werden soll. Nach der Bestätigung wird das Update heruntergeladen, und die neuen Programmkomponenten werden anschließend installiert.

Die Standardoption für Updates für Programmkomponenten ist **Benutzer fragen**.



Nach der Installation eines Updates für Programmkomponenten ist ein Neustart des Systems erforderlich, um die Funktionalität aller Module zu gewährleisten. Im Bereich **Neustart nach Update von Programmkomponenten** kann der Benutzer eine der folgenden drei Optionen auswählen:

- **Kein Neustart**
- **Zur Bestätigung auffordern**
- **Computer automatisch neu starten, ohne Nachfrage**

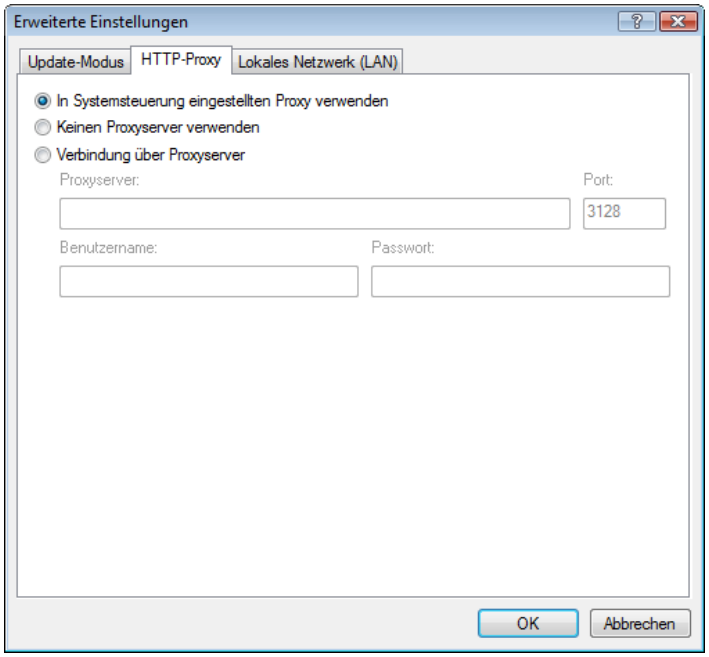
Die Standardeinstellung für den Neustart ist **Zur Bestätigung auffordern**. Die Auswahl der geeigneten Option für Updates für Programmkomponenten auf der Registerkarte **Update-Modus** hängt vom jeweiligen Computer ab, auf dem die Einstellungen zugewiesen werden. Beachten Sie die unterschiedliche Funktion von Arbeitsplatzcomputern und Servern–das automatische Neustarten eines Servers nach einem Update kann schwerwiegende Folgen haben.

4.4.1.2.2 Proxyserver

Um auf die Proxyserver-Einstellungen für ein bestimmtes Update-Profil zuzugreifen, klicken Sie in den erweiterten Einstellungen (F5) auf **Update** und dann auf **Einstellungen...** rechts neben den **erweiterten Update-Einstellungen.** Klicken Sie auf die Registerkarte **HTTP-Proxy**, und wählen Sie eine der folgenden drei Optionen:

- **Allgemeine Einstellungen für den Proxyserver verwenden**
- **Keinen Proxyserver verwenden**
- **Verbindung über Proxyserver** (Verbindung wird durch Verbindungseigenschaften definiert)

Bei Auswahl der Option **Allgemeine Einstellungen für den Proxyserver verwenden** werden die Proxyserver-Konfigurationsoptionen verwendet, die in den erweiterten Einstellungen unter **Allgemein > Proxyserver** angegeben wurden.



Wählen Sie die Option **Keinen Proxyserver verwenden**, wenn Sie festlegen möchten, dass kein Proxyserver für die Aktualisierung von ESET Smart Security verwendet werden soll.

Die Option **Verbindung über Proxyserver** sollte gewählt werden, wenn für die Aktualisierung von ESET Smart Security ein anderer Proxyserver als der in den allgemeinen Einstellungen (**Allgemein > Proxyserver**) angegebene verwendet wird. In diesem Fall sind weitere Einstellungen erforderlich: **Proxyserver**-Adresse, der **Port** für die Datenübertragung sowie **Benutzername** und **Passwort** für den Proxyserver, falls erforderlich.

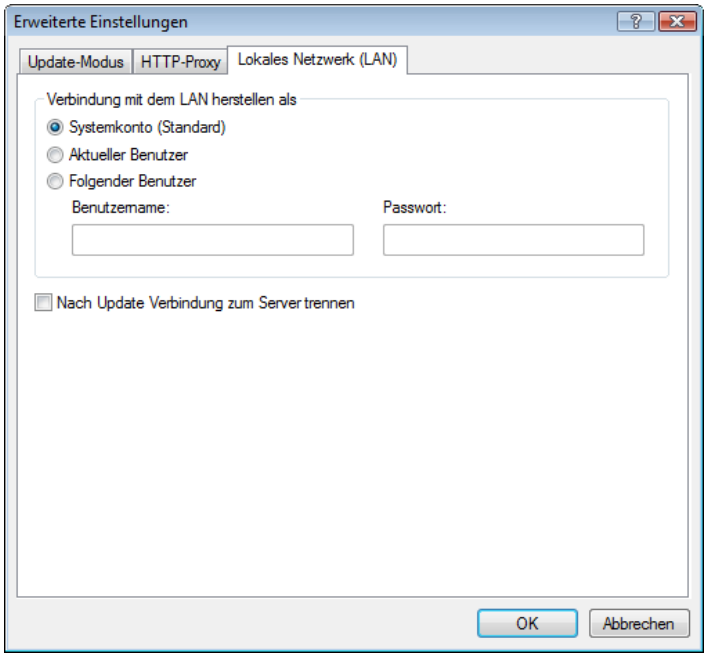
Diese Option sollte auch verwendet werden, wenn in den allgemeinen Einstellungen kein Proxyserver festgelegt wurde, ESET Smart Security jedoch die Verbindung über einen Proxyserver aufbaut.

Die Standardeinstellung für den Proxyserver ist **Allgemeine Einstellungen für den Proxyserver verwenden**.

4.4.1.2.3 LAN-Verbindungen

Beim Aktualisieren von einem lokalen Server unter Windows NT ist standardmäßig eine Authentifizierung für jede Netzwerkverbindung erforderlich. In den meisten Fällen besitzt ein lokales Systemkonto keine ausreichenden Berechtigungen für den Zugriff auf den Mirror-Ordner (der Kopien der Update-Dateien enthält). Geben Sie in diesem Fall den Benutzernamen und das Passwort in den Update-Einstellungen ein, oder geben Sie ein Konto an, über das das Programm auf den Update-Mirror zugreifen kann.

Um ein solches Konto zu konfigurieren, klicken Sie auf die Registerkarte **LAN**. Der Bereich **Verbindung mit dem LAN herstellen als** enthält die Optionen **Systemkonto (Standardeinstellung)**, **Aktueller Benutzer** und **Folgender Benutzer**.



Wählen Sie **Systemkonto**, um das Systemkonto für die Authentifizierung zu verwenden. Normalerweise findet keine Authentifizierung statt, wenn in den Haupteinstellungen für Updates keine Authentifizierungsdaten angegeben sind.

Um sicherzustellen, dass das Programm sich mit dem Konto eines aktuell angemeldeten Benutzers autorisiert, wählen Sie **Aktueller Benutzer**. Nachteil dieser Lösung ist, dass das Programm keine Verbindung zum Update-Server herstellen kann, wenn kein Benutzer angemeldet ist.

Wählen Sie **Folgender Benutzer**, wenn das Programm ein spezielles Benutzerkonto für die Authentifizierung verwenden soll.

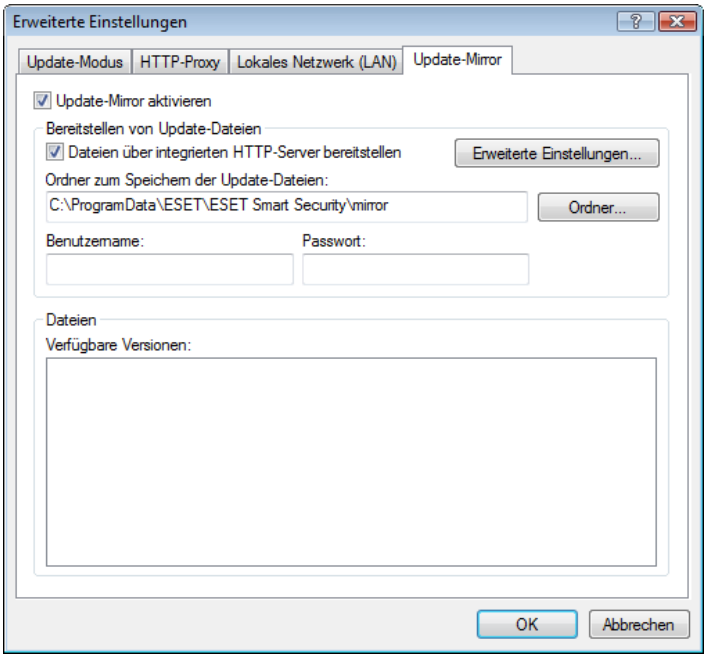
Die Standardeinstellung für LAN-Verbindungen ist **Systemkonto**.

Warnung:
Wenn eine der Optionen **Aktueller Benutzer** oder **Folgender Benutzer** aktiviert ist, kann beim Wechsel der Identität zum gewünschten Benutzer ein Fehler auftreten. Aus diesem Grund wird empfohlen, die LAN-Authentifizierungsdaten in den Haupteinstellungen für Updates einzugeben. In diesen Update-Einstellungen geben Sie die Authentifizierungsdaten wie folgt ein: Domain-Name\Benutzer (bei einer Arbeitsgruppe geben Sie Arbeitsgruppenname\Name ein) und das Benutzerpasswort. Bei der Aktualisierung von der HTTP-Version des lokalen Servers ist keine Authentifizierung erforderlich.

4.4.1.2.4 Erstellen von Update-Kopien–Update-Mirror

Mit ESET Smart Security Business Edition können Kopien der Update-Dateien erstellt werden, die für die Aktualisierung anderer Computer im Netzwerk verwendet werden können. Das Aktualisieren der Clientcomputer von einem Update-Mirror sorgt für eine optimierte Lastenverteilung im Netzwerk sowie eine Reduzierung der benötigten Bandbreiten.

Die Konfigurationsoptionen für den Update-Mirror des lokalen Servers befinden sich im Bereich **Erweiterte Einstellungen Update**. (Dafür müssen Sie zunächst im Lizenzmanager, der sich im Bereich „Erweiterte Einstellungen" von ESET Smart Security Business Edition öffnen lässt, einen gültigen Lizenzschlüssel eingeben. Um auf diesen Bereich zuzugreifen, drücken Sie F5, und klicken Sie unter „Erweiterte Einstellungen" auf **Update**. Klicken Sie auf die Schaltfläche **Einstellungen...** neben **Erweiterte Einstellungen Update:**, und wählen Sie die Registerkarte **Update-Mirror**.)



Der erste Schritt bei der Konfiguration des Update-Mirror besteht in der Aktivierung des Kontrollkästchens **Update-Mirror aktivieren**. Durch das Aktivieren dieser Option stehen weitere Konfigurationsoptionen für Update-Mirror zur Verfügung, die beispielsweise die Art des Zugriffs auf Update-Dateien und den Pfad zu den Kopien der Update-Dateien betreffen.

Die Vorgehensweise zur Aktivierung des Update-Mirror wird im folgenden Kapitel, „Aktualisieren über Update-Mirror", ausführlich beschrieben. Vorläufig sei angemerkt, dass es zwei Grundvarianten des Zugriffs auf den Update-Mirror gibt: Der Ordner mit den Update-Dateien kann eine Netzwerkfreigabe sein, oder es wird ein HTTP-Server als Update-Mirror verwendet.

Der den Update-Dateikopien vorbehaltene Ordner wird im Bereich **Speicherordner für Kopien der Update-Dateien** festgelegt. Klicken Sie auf **Durchsuchen...**, um den gewünschten Ordner auf dem lokalen Computer oder eine Netzwerkfreigabe auszuwählen. Wenn für den angegebenen Ordner eine Authentifizierung erforderlich ist, müssen die Authentifizierungsdaten in die Felder **Benutzername** und **Passwort** eingetragen werden. Der Benutzername muss im Format *Domain/Benutzer* oder *Arbeitsgruppe/Benutzer* eingegeben werden. Denken Sie daran, auch die entsprechenden Passwörter einzugeben.

In den erweiterten Einstellungen für Update-Mirror kann auch die Sprachversion der herunterzuladenden Update-Kopien angegeben werden. Zum Auswählen der Sprache wechseln Sie zu **Dateien–Verfügbare Versionen:**.

4.4.1.2.4.1 Aktualisieren über Update-Mirror

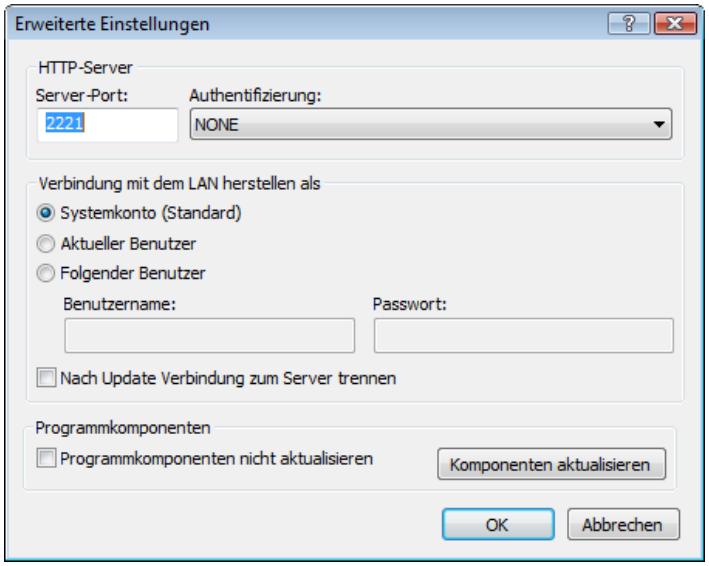
Es gibt zwei Grundvarianten für den Zugriff auf den Update-Mirror: Der Ordner mit den Update-Dateien kann eine Netzwerkfreigabe sein, oder es wird ein HTTP-Server als Update-Mirror verwendet.

Zugriff auf den Update-Mirror über einen internen HTTP-Server

Dies ist die in der vordefinierten Programmkonfiguration festgelegte Standardkonfiguration. Um mit dem HTTP-Server auf den Update-Mirror zugreifen zu können, wechseln Sie zu **Erweiterte Einstellungen Update** (Registerkarte **Update-Mirror**), und markieren Sie die Option **Update-Mirror aktivieren**.

In den **erweiterten Einstellungen** des **Update-Mirror** können Sie den **Server-Port** angeben, auf dem der HTTP-Server Anfragen empfängt, und den Typ der **Authentifizierung** festlegen, die vom HTTP-Server verwendet wird. Standardmäßig weist der Server-Port den Wert **2221** auf. Mit der Option **Authentifzierung** können Sie die für den Zugriff auf die Update-Dateien verwendete Authentifizierungsmethode wählen. Folgende Optionen stehen zur Verfügung: **KEINE, Basic** und **NTLM**. Wählen Sie **Basic** für Base64-Verschlüsselung und einfache Authentifizierung mit Benutzernamen und Passwort. Bei Auswahl von **NTLM** wird eine sichere Verschlüsselungsmethode verwendet. Zur Authentifizierung wird der auf dem Computer erstellte Benutzer verwendet, der die Update-Dateien freigegeben hat. Die Standardeinstellung ist **KEINE**, bei der für den Zugriff auf die Update-Dateien keine Authentifizierung erforderlich ist.

Warnung:
Wenn Sie den Zugriff auf die Update-Dateien über einen HTTP-Server zulassen möchten, muss sich der Ordner mit den Kopien der Update-Dateien auf demselben Computer befinden wie die Instanz von ESET Smart Security, mit der dieser Ordner erstellt wird.



Wenn die Konfiguration des Update-Mirror abgeschlossen ist, fügen Sie auf den einzelnen Computern einen neuen Update-Server hinzu. Das Format lautet: **http://IP-Adresse_Ihres_Servers:2221**. Führen Sie dazu die folgenden Schritte aus:

- Öffnen Sie die **Erweiterten Einstellungen von ESET Smart Security** und klicken Sie auf **Update**.
- Klicken Sie auf **Bearbeiten...** rechts neben dem Dropdown-Menü **Update-Server** und geben Sie den neuen Server im folgenden Format ein: http://IP-Adresse_Ihres_Servers:2221
- Wählen Sie den neu hinzugefügten Server aus der Liste der Update-Server aus.

Zugriff auf den Update-Mirror über Systemfreigaben

Zunächst muss in einem lokalen oder Netzwerklaufwerk ein freigegebener Ordner erstellt werden. Beim Erstellen des Ordners für den Update-Mirror ist Folgendes zu beachten: Der Benutzer, der Update-Dateien im Ordner speichert, benötigt Schreibzugriff, während die Benutzer, die ESET Smart Security über diesen Ordner aktualisieren, eine Leseberechtigung benötigen.

Die Konfiguration des Zugriffs auf den Update-Mirror wird fortgesetzt, indem Sie im Bereich **Erweiterte Einstellungen Update** (Registerkarte **Update-Mirror**) die Option **Dateien bereitstellen über integrierten HTTP-Server** deaktivieren. Diese Option ist in der Standardeinstellung des Programms aktiviert.

Wenn sich der freigegebene Ordner auf einem anderen Computer im Netzwerk befindet, ist für den Zugriff auf diesen Computer eine Authentifizierung erforderlich. Um die Authentifizierungsdaten anzugeben, wechseln Sie in die erweiterten Einstellungen von ESET Smart Security (mit F5), und wählen Sie **Verbindung mit dem LAN herstellen aus**. Klicken Sie auf **Einstellungen...** und anschließend auf die Registerkarte **LAN**. Diese Einstellung entspricht der Einstellung für Updates, wie im Kapitel „Herstellen einer LAN-Verbindung" beschrieben.

Nach Abschluss der Konfiguration des Update-Mirror geben Sie auf den einzelnen Computern jeweils \\UNC\PATH als Update-Server ein. Führen Sie dazu die folgenden Schritte aus:

- Öffnen Sie die erweiterten Einstellungen von ESET Smart Security, und klicken Sie auf **Update**.
- Klicken Sie neben dem Update-Server auf **Bearbeiten...**, und geben Sie den neuen Server im folgenden Format ein: \\UNC\PATH.
- Wählen Sie den neu hinzugefügten Server aus der Liste der Update-Server aus.

HINWEIS:
Um ein fehlerfreies Funktionieren zu gewährleisten, muss der Pfad zum Ordner mit den Kopien der Update-Dateien als UNC-Pfad angegeben werden. Updates über verbundene Netzlaufwerke funktionieren möglicherweise nicht.

4.4.1.2.4.2 Fehlerbehebung bei Updates über Update-Mirror

Je nachdem, welche Methode für den Zugriff auf den Mirror-Ordner verwendet wird, können verschiedene Probleme auftreten. Die meisten Probleme mit Updates von einem Update-Mirror haben eine oder mehrere der folgenden Ursachen: falsche Einstellungen oder Authentifizierungsdaten für den Mirror-Ordner, falsche Konfiguration auf lokalen Computern, die versuchen, Update-Dateien vom Update-Mirror herunterzuladen, oder eine Kombination der angegebenen Gründe. Hier erhalten Sie einen Überblick über die am häufigsten auftretenden Probleme bei Updates von einem Update-Mirror:

- **ESET Smart Security meldet einen Fehler bei der Verbindung mit dem Mirror-Server –** Wahrscheinlich wird dieser Fehler durch falsche Angaben zum Update-Server (Netzwerkpfad zum Mirror-Ordner) verursacht, von dem die lokalen Computer Updates herunterladen. Um den Ordner zu überprüfen, klicken Sie unter Windows auf **Start > Ausführen...**, geben den Ordnernamen ein und klicken auf **OK**. Daraufhin sollte der Inhalt des Ordners angezeigt werden.
- **ESET Smart Security verlangt einen Benutzernamen und ein Passwort –** Es wurden wahrscheinlich falsche Authentifizierungsdaten (Benutzername und Passwort) im Bereich „Update" angegeben. Benutzername und Passwort werden für den Zugriff auf den Update-Server verwendet, über den das Programm aktualisiert wird. Vergewissern Sie sich, dass die Authentifizierungsdaten korrekt und im richtigen Format eingegeben sind. Verwenden Sie das Format *Domain/Benutzername* bzw. *Arbeitsgruppe/Benutzername* und die entsprechenden Passwörter. Auch wenn „alle" auf den Mirror-Server zugreifen können, sollten Sie bedenken, dass deshalb nicht jedem beliebigen Benutzer der Zugriff gewährt wird. „Alle" umfasst keine nicht autorisierten Benutzer, sondern bedeutet, dass alle Benutzer der Domain auf den Ordner zugreifen können. Daher müssen, auch wenn „alle" auf den Ordner zugreifen können, in den Update-Einstellungen ein Domain-Benutzername und -Passwort eingegeben werden.

- **ESET Smart Security meldet einen Fehler bei der Verbindung mit dem Mirror-Server** – Der für den Zugriff auf die HTTP-Version des Update-Mirror angegebene Port ist blockiert.

4.4.2 So erstellen Sie Update-Tasks

Mit der Option **Update der Signaturdatenbank** können Updates manuell ausgeführt werden. Klicken Sie dazu im Hauptmenü auf **Update**, und wählen Sie im Informationsfenster die entsprechende Option aus.

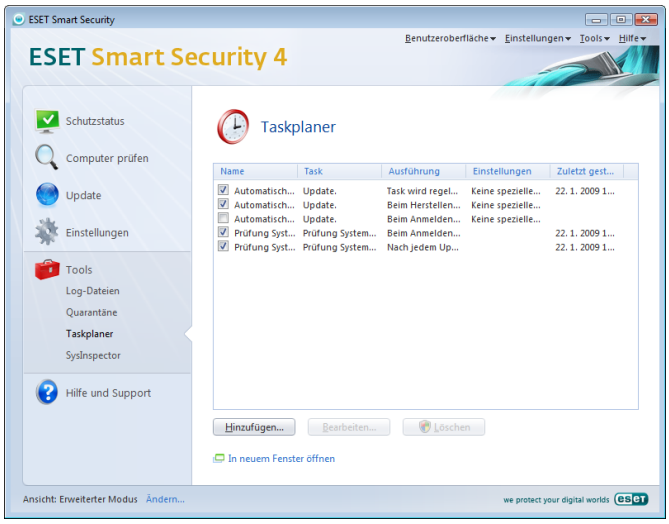
Updates können auch als geplante Vorgänge (Tasks) ausgeführt werden. Die Einstellungen für Tasks finden Sie unter **Extras > Taskplaner**. Standardmäßig sind in ESET Smart Security folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**

Diese Update-Tasks können bei Bedarf bearbeitet werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie im Kapitel „Taskplaner".

4.5 Taskplaner

Der Taskplaner ist bei Aktivierung des erweiterten Modus von ESET Smart Security verfügbar. Der **Taskplaner** kann im Hauptmenü von ESET Smart Security unter **Tools** aufgerufen werden. Der Taskplaner umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Prüfprofils.



Standardmäßig werden im **Taskplaner** die folgenden Tasks angezeigt:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Herstellen von DFÜ-Verbindungen**
- **Automatische Updates beim Anmelden des Benutzers**
- **Prüfung Systemstartdateien nach Anmeldung des Benutzers**
- **Prüfung Systemstartdateien nach Update der Signaturdatenbank**

Um die Konfiguration eines vorhandenen Task (sowohl standardmäßig als auch benutzerdefiniert) zu ändern, klicken Sie mit der rechten Maustaste auf den Task und dann auf **Bearbeiten...**, oder wählen Sie den Task aus, den Sie ändern möchten, und klicken Sie auf **Bearbeiten...**.

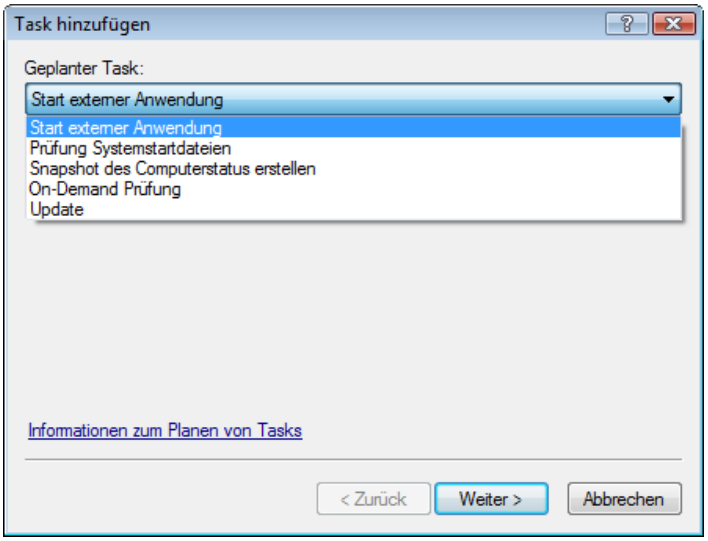
4.5.1 Verwendung von Tasks

Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften. Konfiguration und Eigenschaften enthalten Informationen wie Datum und Uhrzeit sowie bestimmte Profile, die bei Ausführung des Task verwendet werden.

4.5.2 Erstellen von Tasks

Zum Erstellen eines Task im Taskplaner klicken Sie mit der rechten Maustaste auf **Hinzufügen...**, oder wählen Sie im Kontextmenü die Option **Hinzufügen...**. Es gibt fünf Arten von Tasks:

- **Anwendung starten**
- **Log-Wartung**
- **Prüfung Systemstartdateien**
- **Manuelles Prüfen des Computers**
- **Update**



Da **Manuelles Prüfen des Computers** und **Update** die meistverwendeten Tasks sind, wird hier das Hinzufügen eines neuen Update-Task beschrieben.

Wählen Sie im Dropdown-Menü **Task:** die Option **Update**. Klicken Sie auf **Weiter**, und geben Sie den Namen des Task in das Feld **Taskname:** ein. Wählen Sie die Häufigkeit des Task. Folgende Optionen stehen zur Verfügung: **Einmalig, Wiederholt, Täglich**, **Wöchentlich** und **Bei Ereignis**. Je nach ausgewählter Frequenz werden Ihnen verschiedene Update-Parameter angezeigt. Im nächsten Schritt können Sie eine Aktion festlegen für den Fall, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann. Folgende Optionen stehen zur Verfügung:

- **Nächste Ausführung genau nach Planung**
- **Ausführung zum nächstmöglichen Zeitpunkt**
- **Task sofort ausführen, wenn die Zeit seit der letzten Ausführung das festgelegte Intervall überschreitet** (das Intervall kann über das Feld **Taskzeitraum** festgelegt werden)

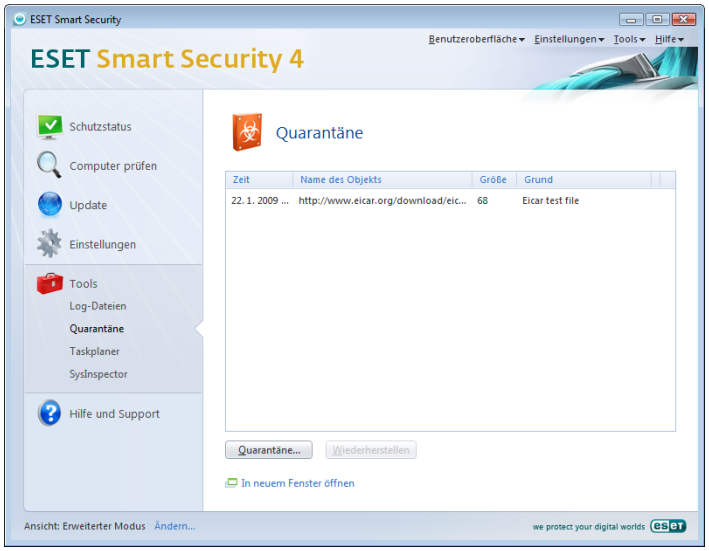
Anschließend wird eine Zusammenfassung des aktuellen Task angezeigt. Die Option **Task mit speziellen Einstellungen ausführen** sollte automatisch aktiviert sein. Klicken Sie auf **Fertig stellen**.

Es wird ein Dialogfenster angezeigt, in dem Profile für den Task ausgewählt werden können. Hier können ein primäres und ein alternatives Profil festgelegt werden. Letzteres wird verwendet, falls der Task unter Verwendung des primären Profils nicht abgeschlossen werden kann. Bestätigen Sie Ihre Angaben, indem Sie im Fenster **Update-Profile** auf **OK** klicken. Der neue Task wird der Liste der aktuellen Tasks hinzugefügt.

4.6 Quarantäne

Die wichtigste Aufgabe der Quarantäne ist die sichere Speicherung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Smart Security fälschlicherweise erkannt worden sind.

Es können beliebige Dateien unter Quarantäne gestellt werden. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, bei der Virenprüfung jedoch nicht erkannt werden. Dateien in Quarantäne können zur Analyse an ESET gesendet werden.



Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (**Hinzugefügt durch Benutzer...**) und die Anzahl der Bedrohungen (z. B. bei Archiven, in denen an mehreren Stellen Schadcode erkannt wurde) enthält.

4.6.1 Quarantäne für Dateien

Das Programm kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Auf Wunsch können Sie beliebige verdächtige Dateien manuell in die Quarantäne verschieben, indem Sie auf **Quarantäne...** klicken. In diesem Fall wird die Originaldatei nicht von ihrem ursprünglichen Speicherort entfernt. Zu diesem Zweck kann auch das Kontextmenü verwendet werden. Klicken Sie mit der rechten Maustaste in das Quarantänefenster, und wählen Sie **Hinzufügen...**

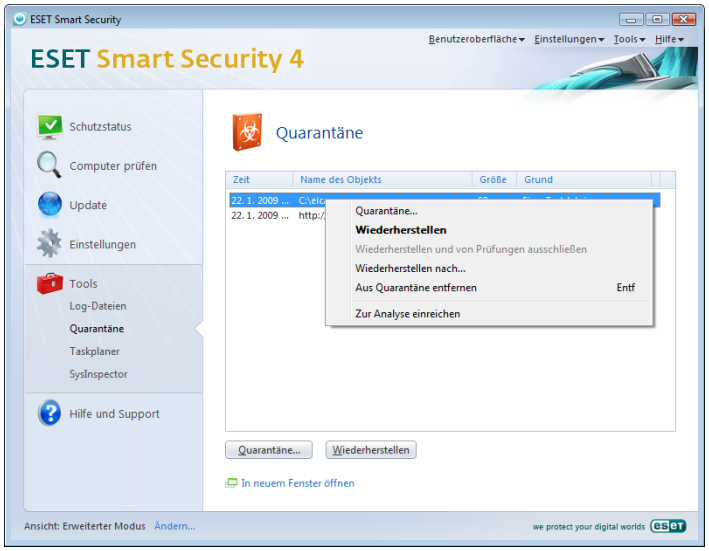
4.6.2 Wiederherstellen aus der Quarantäne

Dateien in Quarantäne können auch an ihrem ursprünglichen Speicherort wiederhergestellt werden. Verwenden Sie dazu die Funktion **Wiederherstellen** im Kontextmenü, das angezeigt wird, wenn Sie im Quarantänefenster mit der rechten Maustaste auf die entsprechende Datei klicken. Das Kontextmenü enthält auch die Option **Wiederherstellen nach**, mit der Dateien an einem anderen als ihrem ursprünglichen Speicherort wiederhergestellt werden können.

HINWEIS:
Wenn versehentlich eine harmlose Datei in Quarantäne versetzt wurde, schließen Sie die Datei nach der Wiederherstellung von der Prüfung aus, und senden Sie sie an den ESET-Kundendienst.

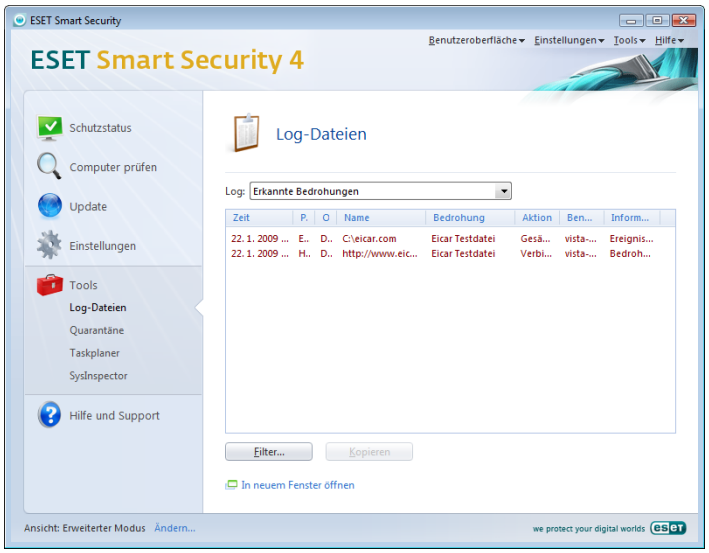
4.6.3 Senden von Dateien in Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an ESET. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie im angezeigten Kontextmenü die Option **Zur Analyse senden**.



4.7 Log-Dateien

Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Erstellen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Problemen oder Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET Smart Security heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.



Log-Dateien können über das Hauptfenster von ESET Smart Security aufgerufen werden, indem Sie auf **Tools > Log-Dateien** klicken.

Wählen Sie oben im Fenster mithilfe des Dropdown-Menüs **Log:** den gewünschten Log-Typ aus. Folgende Logs sind verfügbar:

1. **Erkannte Bedrohungen –** Über diese Option können Sie sämtliche Informationen über Ereignisse bezüglich der Erkennung eingedrungener Schadsoftware anzeigen.

2. **Ereignisse –** Diese Option kann von Systemadministratoren und Benutzern zur Lösung von Problemen verwendet werden. Alle von ESET Smart Security ausgeführten wichtigen Aktionen werden in den Ereignis-Logs aufgezeichnet.

3. **Manuelles Prüfen des Computers –** In diesem Fenster werden die Ergebnisse aller durchgeführten Prüfungen angezeigt. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu der entsprechenden manuellen Prüfung anzeigen.

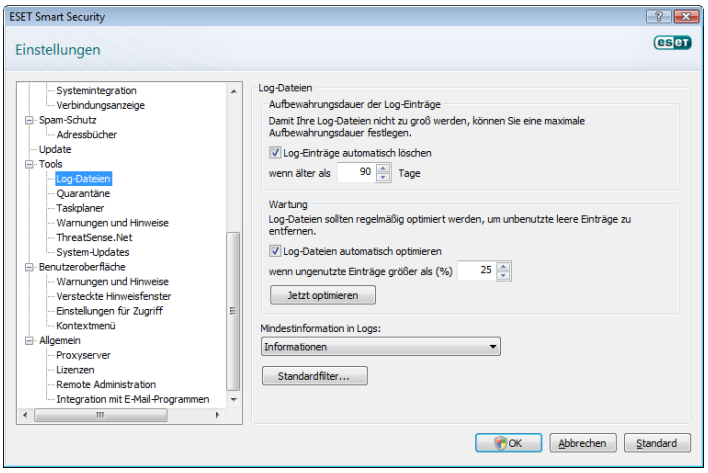
4. **Log von ESET Personal Firewall –** Dieses Log enthält die Aufzeichnungen aller von der Personal Firewall erkannten Daten und andere die Firewall betreffenden Informationen. Durch eine Analyse des Firewall-Logs können Versuche, in das System einzudringen, rechtzeitig erkannt werden.

In jedem Abschnitt können die angezeigten Informationen direkt in die Zwischenablage kopiert werden. Dazu wählen Sie die gewünschten Einträge aus und klicken auf **Kopieren**. Um mehrere Einträge auszuwählen, können Sie die Taste STRG und die Umschalttaste verwenden.

4.7.1 Log-Wartung

Die Log-Einstellungen können über das Hauptfenster von ESET Smart Security aufgerufen werden. Klicken Sie auf **Einstellungen > Erweiterte Einstellungen... > Tools > Log-Dateien**. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

- **Log-Einträge automatisch löschen:** Log-Einträge, die länger als angegeben gespeichert sind, werden automatisch gelöscht.
- **Log-Dateien automatisch optimieren:** Die Logs werden beim Erreichen des vordefinierten Fragmentierungsgrads automatisch optimiert.
- **Ausführlichkeit der Logs, mindestens:** Hier können Sie angeben, wie ausführlich die Logs sein sollen. Verfügbare Optionen:
  - **Kritische Fehler–**Nur kritische Fehler werden protokolliert (Fehler beim Starten des Virenschutzes, der Personal Firewall usw.)
  - **Fehler –** Einfache Fehler wie „Fehler beim Herunterladen einer Datei" und kritische Fehler werden protokolliert.
  - **Warnungen –** Kritische Fehler und Warnungen werden protokolliert.
  - **Hinweise –** Alle Hinweise, Warnungen und Fehler werden protokolliert.
  - **Ereignismeldungen –** Alle bisher genannten Meldungen und alle sonstigen Meldungen, die für das Beheben von Fehlern wichtig sein können, werden protokolliert.



4.8 Benutzeroberfläche

Die Benutzeroberfläche von ESET Smart Security lässt sich so konfigurieren, dass die Arbeitsumgebung den Bedürfnissen des Benutzers entspricht. Auf die Konfigurationsoptionen kann über die **Benutzeroberfläche** der erweiterten Einstellungen von ESET Smart Security zugegriffen werden.

Mit den **Elementen der Benutzeroberfläche** kann der erweiterte Modus ein- und ausgeschaltet werden. Im erweiterten Modus werden erweiterte Einstellungen und zusätzliche Steuerelemente für ESET Smart Security angezeigt.

Die **Grafische Benutzeroberfläche** sollte deaktiviert werden, wenn durch die grafischen Elemente die Leistung des Computers beeinträchtigt wird oder andere Probleme auftreten. Auch bei sehbehinderten Benutzern kann die grafische Oberfläche deaktiviert werden, da Konflikte mit Spezialanwendungen zum Lesen von Text auf dem Bildschirm auftreten können.

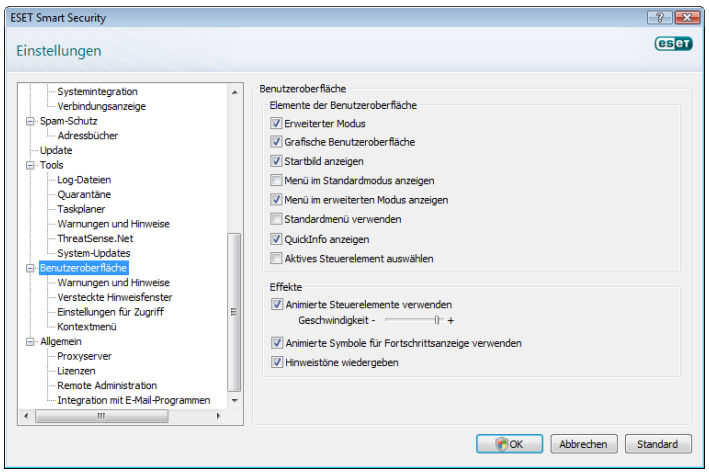
Wenn ESET Smart Security ohne Anzeige des Startbilds gestartet werden soll, deaktivieren Sie die Option **Startbild anzeigen**.

Oben im Hauptfenster von ESET Smart Security befindet sich ein Standardmenü, das mit der Option **Standardmenü verwenden** aktiviert oder deaktiviert werden kann.

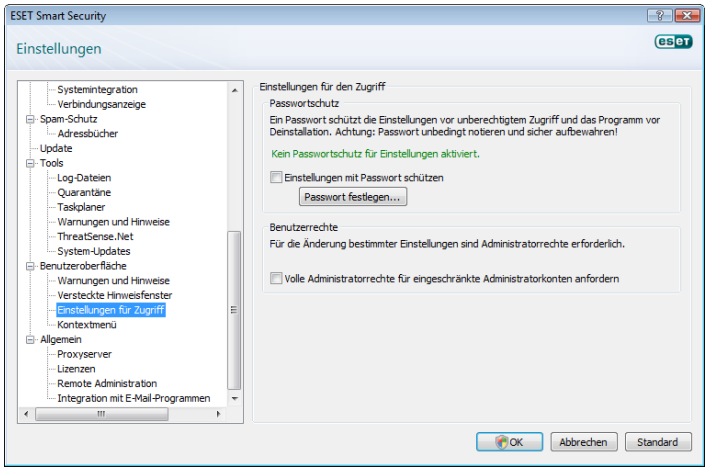
Wenn die Option **Quickinfo anzeigen** aktiviert ist, wird für jede Option, über die der Mauszeiger bewegt wird, eine kurze Beschreibung angezeigt. Mit der Option **Aktives Steuerelement auswählen** wird jedes Element hervorgehoben, das sich im aktiven Bereich des Mauszeigers befindet. Das hervorgehobene Element kann durch einen Mausklick aktiviert werden.

Um die Geschwindigkeit der animierten Effekte zu steigern oder zu reduzieren, wählen Sie die Option **Animierte Steuerelemente verwenden**, und bewegen Sie den Schieber **Geschwindigkeit** nach rechts oder links.

Um animierte Symbole zur Darstellung des Fortschritts von Aktivitäten zu verwenden, markieren Sie die Option **Animierte Symbole verwenden...**. Wenn das Programm bei wichtigen Ereignissen einen Warnton abgeben soll, markieren Sie die Option **Hinweistöne wiedergeben**.



Im Bereich **Benutzeroberfläche** befindet sich auch eine Option, um die Einstellungen von ESET Smart Security mit einem Passwort zu schützen. Sie wird über das Untermenü **Einstellungen schützen** der **Benutzeroberfläche** aufgerufen. Maßgeblich für einen wirksamen Schutz Ihres Systems sind die korrekten Einstellungen des Programms. Bei unzulässigen Änderungen können wichtige Daten verloren gehen. Um ein Passwort zum Schutz der Einstellungen einzurichten, klicken Sie auf **Passwort eingeben...**



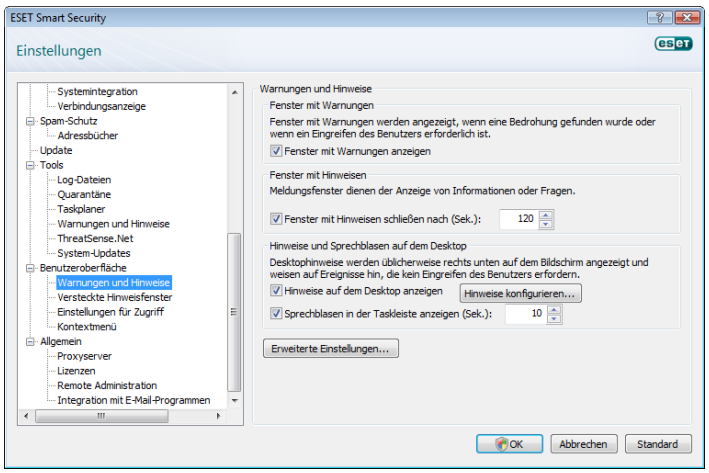
4.8.1 Warnungen und Hinweise

Unter **Benutzeroberfläche** können Sie im Bereich **Einstellungen für Warnungen und Hinweise** konfigurieren, wie Warnungen und Systemmeldungen in ESET Smart Security 4 behandelt werden sollen.

Die erste Option ist **Warnungen anzeigen**. Bei Deaktivieren dieser Option werden keine Warnmeldungen mehr angezeigt. Diese Einstellung eignet sich nur in einigen speziellen Situationen. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten.

Wenn Popup-Fenster nach einer bestimmten Zeit automatisch geschlossen werden sollen, aktivieren Sie die Option **Hinweise automatisch schließen (Sek.)**. Die Hinweise werden nach Ablauf einer bestimmten Zeit automatisch geschlossen, sofern sie nicht bereits vom Benutzer manuell geschlossen worden sind.

Hinweise auf dem Desktop und Sprechblasen dienen ausschließlich zu Informationszwecken. Eingaben des Benutzers sind weder möglich noch erforderlich. Die Hinweise und Sprechblasen werden im Hinweisbereich rechts unten auf dem Bildschirm angezeigt. Zum Aktivieren der Anzeige von Desktophinweisen aktivieren Sie die Option **Hinweise auf dem Desktop anzeigen**. Weitere Optionen, wie Anzeigedauer und Transparenz, lassen sich einstellen, indem Sie auf **Einstellungen...** klicken. Um eine Vorschau des Verhaltens von Meldungen zu erhalten, klicken Sie auf **Vorschau**. Die Anzeigedauer von Sprechblasen lässt sich über die Option **Sprechblasen in der Taskleiste anzeigen (Sek.)** einstellen.



Klicken Sie auf **Erweiterte Einstellungen...**, um zusätzliche Einstellungen für **Warungen und Hinweise** einzugeben, einschließlich **Nur Meldungen anzeigen, die ein Eingreifen des Benutzers erfordern**. Hiermit können Sie die Anzeige von Meldungen, die keine Benutzerinteraktion erfordern, aktivieren bzw. deaktivieren. Wählen Sie die Option „Nur Meldungen anzeigen, die ein Eingreifen des Benutzers erfordern" aus, um alle nicht-interaktiven Benachrichtigungen zu unterdrücken, wenn Sie Anwendungen im Vollbildmodus ausführen. Im Dropdown-Menü zu den anzuzeigenden Mindestinformationen für Ereignisse können Sie den Startschweregrad von anzuzeigenden Warnungen und Benachrichtigungen auswählen.

Der letzte Eintrag in diesem Bereich gibt Ihnen die Möglichkeit, Adressen für Meldungen in einer Mehrbenutzerumgebung anzugeben. Im Feld **Auf Mehrbenutzersystemen Meldungen auf Bildschirm folgenden Benutzers ausgeben:** können Benutzer festlegen, wem wichtige Benachrichtigungen von ESET Smart Security 4 angezeigt werden. Im Normalfall ist dies ein System- oder Netzwerkadministrator. Besonders sinnvoll ist diese Option bei Terminalservern, vorausgesetzt, alle Systemmeldungen werden an den Administrator gesendet.

4.9 ThreatSense.Net

Dank des ThreatSense.Net-Frühwarnsystems erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuer Schadsoftware. Das ThreatSense.Net-Frühwarnsystem funktioniert in zwei Richtungen, hat jedoch nur einen Zweck: die Verbesserung des Schutzes, den wir Ihnen bieten. Die einfachste Möglichkeit, neue Bedrohungen zu erkennen, sobald sie in Erscheinung treten, besteht darin, so viele Kunden wie möglich zu „verknüpfen" und als Virenscouts einzusetzen. Als Benutzer haben Sie zwei Möglichkeiten:

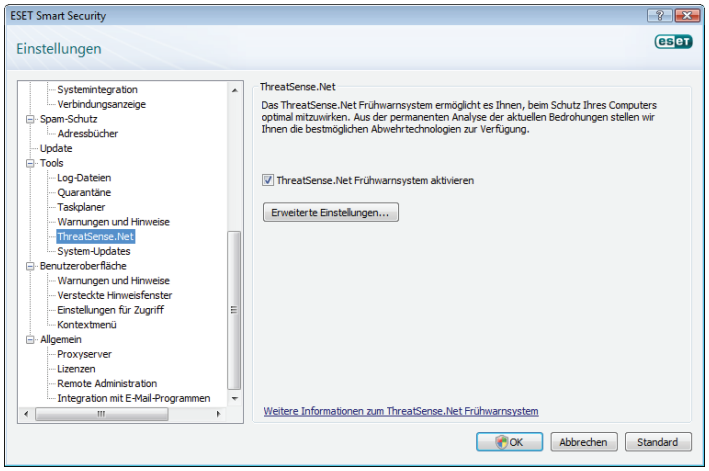
- Sie können sich entscheiden, das ThreatSense.Net-Frühwarnsystem nicht zu aktivieren. Es steht Ihnen der volle Funktionsumfang der Software zur Verfügung, und Sie erhalten auch in diesem Fall den bestmöglichen Schutz.
- Sie können das Frühwarnsystem so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Die Informationen bleiben anonym und werden in einer einzelnen Datei gesendet. Diese Datei kann zur detaillierten Analyse an ESET gesendet werden. Durch die Untersuchung dieser Bedrohungen kann ESET die Fähigkeit seiner Software zur Erkennung von Schadsoftware aktualisieren und verbessern. Das ThreatSense.Net-Frühwarnsystem sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt worden sind. Dazu können auch Proben oder Kopien einer Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der

Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers. Manche dieser Informationen können persönliche Daten über den Benutzer des Computers enthalten, zum Beispiel Benutzernamen in einem Verzeichnispfad usw.

Auch wenn es möglich ist, dass ESET auf diese Weise gelegentlich einige Informationen über Sie oder Ihren Computer erhält, werden diese Daten für KEINEN anderen Zweck als zur Verbesserung der unmittelbaren Reaktion auf Bedrohungen verwendet.

In der Standardeinstellung von ESET Smart Security müssen Sie das Senden verdächtiger Dateien zur genauen Analyse an ESET bestätigen. Beachten Sie, dass Dateien mit bestimmten Endungen wie .doc oder .xls stets von der Übermittlung ausgenommen sind, auch wenn eine Bedrohung darin erkannt wird. Sie können andere Dateierweiterungen hinzufügen, wenn es bestimmte Dateitypen gibt, die Sie oder Ihr Unternehmen nicht übermitteln möchten.

Die Einstellungen für ThreatSense.Net befinden sich in den erweiterten Einstellungen, unter **Tools > ThreatSense.Net**. Markieren Sie das Kontrollkästchen **ThreatSense.Net-Frühwarnsystem aktivieren**. So wird die Funktion aktiviert. Klicken Sie anschließend auf **Erweiterte Einstellungen...**.

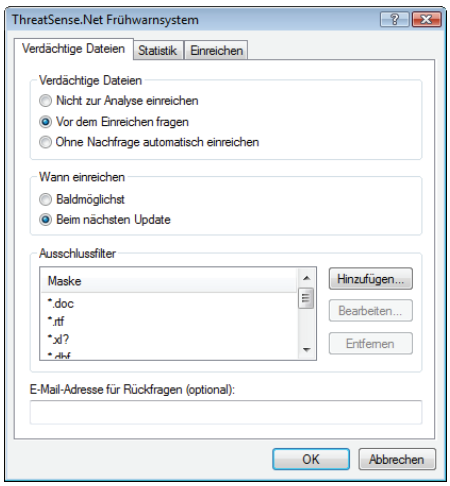


4.9.1 Verdächtige Dateien

Die Registerkarte **Verdächtige Dateien** enthält Einstellungen für das Senden von zu analysierenden Dateien an ESET.

Wenn Ihnen eine Datei verdächtig erscheint, können Sie uns diese zur Analyse senden. Sollte dabei schädlicher Code zutage treten, wird dieser beim nächsten Update der Signaturdatenbank berücksichtigt.

Das Einreichen von Dateien kann automatisch und ohne Nachfrage ausgeführt werden. Bei Aktivierung dieser Option werden die Dateien im Hintergrund versendet. Wenn Sie wissen möchten, welche Dateien zur Analyse gesendet werden, und das Senden bestätigen möchten, wählen Sie die Option **Vor dem Senden fragen**.



Wenn keine Dateien gesendet werden sollen, wählen Sie **Nicht zur Analyse senden**. Beachten Sie, dass das Nichteinsenden von Dateien zur Analyse keine Auswirkungen auf die Übermittlung statistischer Informationen an ESET hat. Die statistischen Informationen werden in einem eigenen Bereich konfiguriert, der im folgenden Kapitel beschrieben wird.

Wann senden
Verdächtige Dateien werden so schnell wie möglich zur Analyse an ESET gesendet. Diese Einstellung wird empfohlen, wenn eine dauerhafte Internetverbindung besteht und die verdächtigen Dateien ohne Verzögerung übermittelt werden können. Die andere Option besteht darin, verdächtige Dateien **Beim nächsten Update** zu senden. In diesem Fall werden die verdächtigen Dateien gesammelt und während eines Updates auf die Server des Frühwarnsystems geladen.

Ausschlussfilter
Nicht alle Dateien müssen zur Analyse versendet werden. Über den Ausschlussfilter können Sie bestimmte Dateien oder Ordner vom Senden ausschließen. Hier können Dateien eingetragen werden, die potenziell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen. Einige typische Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (Microsoft Office, OpenOffice). Die Liste der ausgeschlossenen Dateien kann beliebig erweitert werden.

E-Mail-Adresse
Ihre E-Mail-Adresse wird zusammen mit den verdächtigen Dateien an ESET gesendet und kann dazu verwendet werden, Sie bei Fragen zu kontaktieren. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

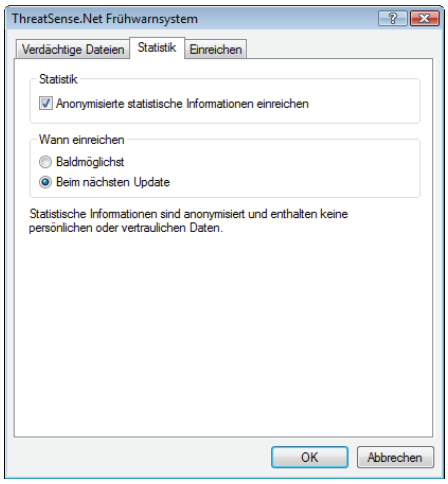
4.9.2 Statistik

Das ThreatSense.Net-Frühwarnsystem sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Erfasst werden der Name der Bedrohung, Datum und Uhrzeit der Erkennung, die Versionsnummer von ESET Smart Security sowie Versionsdaten und die Regionaleinstellung des Betriebssystems. Statistikpakete werden normalerweise einmal oder zweimal täglich an ESET übermittelt.

Beispiel für ein typisches Statistikpaket:

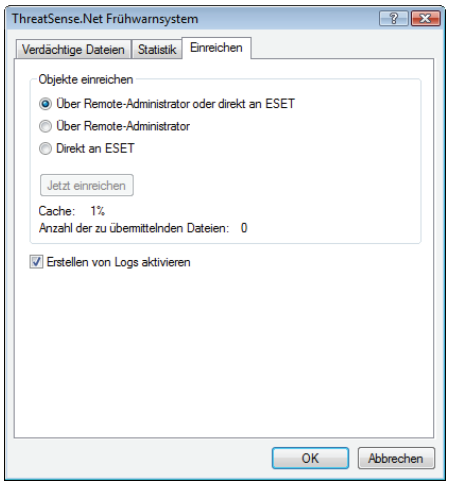
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

Wann einreichen
Im Bereich **Wann einreichen** können Sie festlegen, wann statistische Daten gesendet werden. Wenn Sie die Option **Baldmöglichst** auswählen, werden die statistischen Daten direkt nach ihrer Erstellung gesendet. Diese Einstellung eignet sich, wenn eine dauerhafte Internetverbindung besteht. Bei der Option **Beim nächsten Update** werden die statistischen Daten gespeichert und beim nächsten Update gesammelt gesendet.



4.9.3 Senden

In diesem Bereich können Sie auswählen, ob Dateien und statistische Daten über ESET Remote Administrator oder direkt an ESET gesendet werden. Um sicherzugehen, dass verdächtige Dateien und statistische Informationen an ESET übermittelt werden, wählen Sie **Über Remote Administrator oder direkt an ESET**. Dateien und statistische Daten werden bei Auswahl dieser Option auf jeden Fall übermittelt. Beim Senden verdächtiger Dateien über Remote Administrator werden Dateien und Statistik an den Remote Administration Server gesendet, der sie an ESET weiterleitet. Bei Auswahl der Option **Direkt an ESET** werden alle verdächtigen Dateien und statistischen Daten direkt aus dem Programm an ESET gesendet.



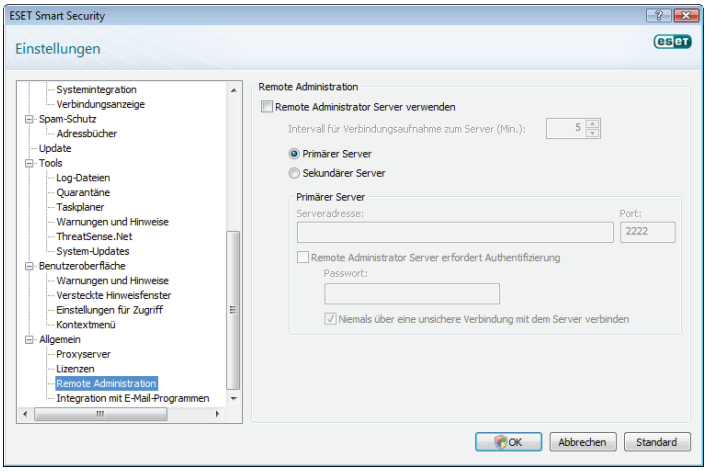
Wenn Dateien vorhanden sind, die noch gesendet werden müssen, ist die Schaltfläche **Jetzt senden** in diesem Einstellungsfenster aktiviert. Klicken Sie auf diese Schaltfläche, um die Dateien und statistischen Daten direkt zu senden.

Aktivieren Sie die Option **Erstellen von Logs aktivieren**, um Informationen über das Senden von Dateien und statistischen Daten aufzuzeichnen. Bei jeder Übertragung einer verdächtigen Datei oder statistischer Informationen wird ein Eintrag im Log erstellt.

4.10 Remoteverwaltung

Die Remoteverwaltung ist ein leistungsfähiges Tool, um Sicherheitsrichtlinien umzusetzen und einen Überblick über die Sicherheit im gesamten Netzwerk zu erhalten. Als besonders sinnvoll erweist sie sich bei größeren Netzwerken. Die Remoteverwaltung bringt nicht nur ein höheres Maß an Sicherheit mit sich, sondern ermöglicht auch die benutzerfreundliche Verwaltung von ESET Smart Security auf Clientcomputern.

Die Optionen des Dialogfensters „Remoteverwaltung" können über das Hauptfenster von ESET Smart Security aufgerufen werden. Klicken Sie auf **Einstellungen > Erweiterte Einstellungen... > Allgemein > Remoteverwaltung**.



Im Fenster „Einstellungen" können Sie die Remoteverwaltung aktivieren, indem Sie das Kontrollkästchen **Remote Administrator Server verwenden** aktivieren. Anschließend können Sie auf folgende Optionen zugreifen:

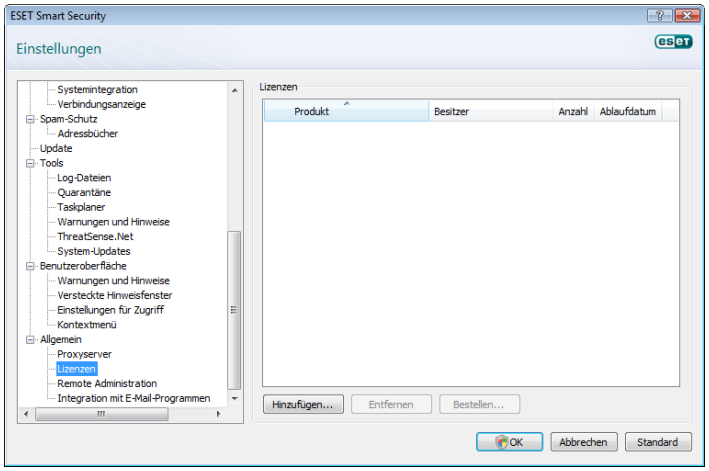
- **Serveradresse –** Netzwerkadresse des Servers, auf dem der Remoteverwaltungsserver installiert ist.
- **Port –** Dieses Feld enthält einen vordefinierten Port für die Verbindung mit dem Server. Es wird empfohlen, den voreingestellten Port 2222 zu verwenden.
- **Intervall für Verbindungsaufnahme zum Server (Min.) –** Hier wird die Häufigkeit angegeben, mit der ESET Smart Security eine Verbindung zum ERA-Server herstellt, um Daten zu übertragen. Mit anderen Worten, die Daten werden in den hier festgelegten Zeitabständen gesendet. Bei der Einstellung 0 werden alle 5 Sekunden Daten gesendet.
- **Remote Administrator Server erfordert Authentifizierung –** Falls erforderlich, können Sie hier ein Passwort für die Verbindung zum Remoteverwaltungsserver eingeben.

Klicken Sie auf **OK** , um die geänderten Einstellungen zu übernehmen. ESET Smart Security nutzt diese Einstellungen zum Verbinden mit dem Remote-Server.

4.11 Lizenz

Unter **Lizenz** werden die Lizenzschlüssel für ESET Smart Security und andere ESET-Produkte wie ESET Remote Administrator und ESET NOD32 für Microsoft Exchange usw. verwaltet. Nach dem Erwerb erhalten Sie die Lizenzschlüssel zusammen mit Ihrem Benutzernamen und dem Passwort. Klicken Sie auf die Schaltflächen **Hinzufügen/Entfernen**, um Lizenzen hinzuzufügen bzw. zu entfernen. Der Lizenzmanager befindet sich in den erweiterten Einstellungen unter **Allgemein > Lizenzen.**

5. Erfahrene Benutzer



Beim Lizenzschlüssel handelt es sich um eine Textdatei mit Informationen zum erworbenen Produkt: Eigentümer, Anzahl der Lizenzen und Ablaufdatum.

Im Fenster „Lizenzmanager" kann der Inhalt eines Lizenzschlüssels geladen und angezeigt werden. Durch Klicken auf **Hinzufügen...** werden die in der Datei enthaltenen Informationen im Lizenzmanager angezeigt. Um Lizenzdateien aus der Liste zu löschen, wählen Sie **Entfernen**.

Wenn ein Lizenzschlüssel abgelaufen ist und Sie die Lizenz erneuern möchten, klicken Sie auf **Bestellen...** Sie werden zu unserem Online-Shop weitergeleitet.

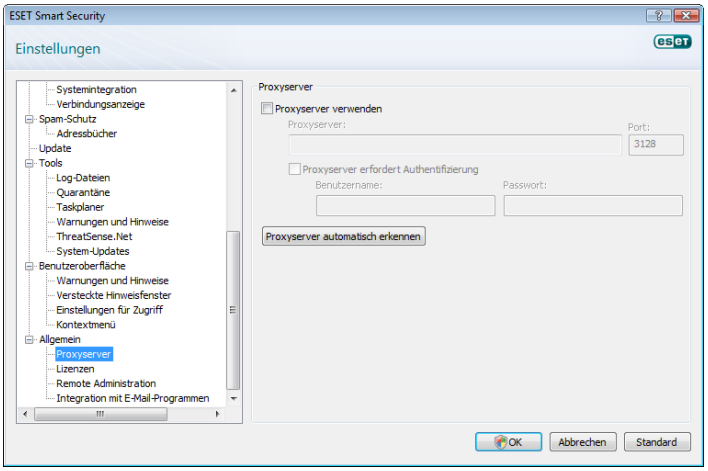
In diesem Kapitel werden Funktionen von ESET Smart Security beschrieben, die besonders für erfahrene Benutzer geeignet sind. Die entsprechenden Optionen stehen ausschließlich im erweiterten Modus zur Verfügung. Um in den erweiterten Modus zu wechseln, klicken Sie im Hauptfenster des Programms links unten auf **Erweiterter Modus Ein/Aus**, oder drücken Sie STRG + M.

5.1 Einstellungen für den Proxyserver

Bei ESET Smart Security kann die Konfiguration des Proxyservers in zwei unterschiedlichen Bereichen der erweiterten Einstellungen vorgenommen werden.

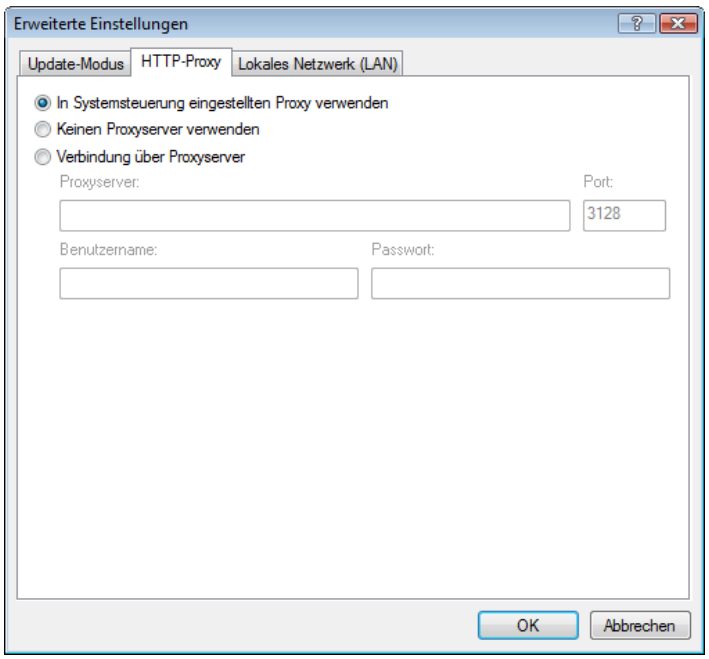
Zum einen können Sie die Einstellungen des Proxyservers unter **Allgemein > Proxyserver** konfigurieren. Dadurch werden die allgemeinen Einstellungen des Proxyservers für ganz ESET Smart Security übernommen. Die Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet benötigen.

Um die Einstellungen des Proxyservers für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Folgenden Proxyserver verwenden**, und geben Sie im Feld **Proxyserver:** die entsprechende Adresse zusammen mit der **Port**nummer des Proxyservers ein.



Wenn der Proxyserver eine Authentifizierung benötigt, aktivieren Sie das Kontrollkästchen **Proxyserver erfordert Authentifizierung**, und geben Sie einen gültigen **Benutzernamen** sowie das entsprechende **Passwort** ein. Klicken Sie auf die Schaltfläche **Proxyserver automatisch erkennen**, wenn die Einstellungen des Proxyservers automatisch erkannt und ausgefüllt werden sollen. Dann werden die Parameter aus dem Internet Explorer kopiert. Beachten Sie, dass mithilfe dieser Funktion keine Authentifizierungsdaten (Benutzername und Passwort) abgerufen werden. Diese müssen vom Benutzer selbst eingegeben werden.

Die Konfiguration des Proxyservers kann aber auch in den **Erweiterten Einstellungen Update** (Option **Update** der erweiterten Einstellungen) vorgenommen werden. Diese Einstellungen gelten für das aktuelle Update-Profil und werden für Laptops empfohlen, da diese die Updates der Virensignaturen häufig von verschiedenen Standorten beziehen. Mehr Informationen zu diesen Einstellungen erhalten Sie im Abschnitt 4.4 „Aktualisierung des Systems".



5.2 Einstellungen exportieren/importieren

Die aktuelle Konfiguration von ESET Smart Security kann im erweiterten Modus unter **Einstellungen**exportiert bzw. importiert werden.

Für Im- und Exporte wird der Dateityp .xml verwendet. Importe und Exporte sind dann hilfreich, wenn Sie die aktuelle Konfiguration von ESET Smart Security zur späteren Verwendung sichern möchten (aus unterschiedlichen Gründen). Die Funktion zum Export der Einstellungen werden vor allem jene zu schätzen wissen, die ihre bevorzugte Konfiguration von ESET Smart Security auf verschiedene Computer übertragen möchten: Sie müssen lediglich die entsprechende .xml-Datei importieren.

5.2.1 Einstellungen exportieren

Die Konfiguration lässt sich problemlos exportieren. Wenn Sie die aktuellen Einstellungen von ESET Smart Security speichern möchten, klicken Sie auf **Einstellungen > Einstellungen importieren und exportieren...**. Markieren Sie die Option **Einstellungen exportieren**, und geben Sie den Namen der Konfigurationsdatei ein. Suchen Sie mithilfe des Browsers einen Speicherort auf Ihrem Computer aus, an dem Sie die Konfigurationsdatei speichern möchten.

5.2.2 Einstellungen importieren

Der Import von Einstellungen verläuft sehr ähnlich. Wählen Sie erneut **Einstellungen importieren und exportieren**, und markieren Sie die Option **Einstellungen importieren**. Klicken Sie auf die Schaltfläche **...**, und suchen Sie nach der Konfigurationsdatei, die Sie importieren möchten.

5.3 Kommandozeile

Das Virenschutz-Modul von ESET Smart Security kann über die Kommandozeile gestartet werden – entweder manuell (mit dem Befehl „ecls") oder über eine Batch-Datei („.bat").

Folgende Parameter und Switches stehen zur Verfügung, um die manuelle Prüfung über die Kommandozeile auszuführen:

Allgemeine Befehle:

– help	Hilfe anzeigen und verlassen
– version	Versionsinformationen anzeigen und verlassen
– base-dir = FOLDER	Module aus FOLDER laden
– quar-dir = FOLDER	Quarantäneordner (FOLDER) angeben
– aind	Aktivitätsanzeige anzeigen

Zu prüfende Objekte:

– files	Dateien prüfen (Standardeinstellung)
– no-files	Dateien nicht prüfen
– boots	Bootsektoren prüfen (Standardeinstellung)
– no-boots	Bootsektoren nicht prüfen
– arch	Archive prüfen (Standardeinstellung)
– no-arch	Archive nicht prüfen
– max-archive-level = LEVEL	Maximale Verschachtelungsebene (LEVEL) bei Archiven
– scan-timeout = LIMIT	Archive maximal für LIMIT (Sekunden) prüfen Wenn die angegebene Prüfzeit abgelaufen ist, wird die Prüfung des Archivs abgebrochen und mit der Prüfung der nächsten Datei fortgesetzt
– max-arch-size=SIZE	Bei Archiven nur die ersten SIZE-Bytes prüfen (Standard: 0 = unbegrenzt)
– mail	E-Mail-Dateien prüfen
– no-mail	E-Mails nicht prüfen
– sfx	Selbstentpackende Archive prüfen
– no-sfx	Selbstentpackende Archive nicht prüfen
– rtp	Laufzeitkomprimierte Dateien prüfen
– no-rtp	Laufzeitkomprimierte Dateien nicht prüfen
– exclude = FOLDER	FOLDER von Prüfung ausnehmen
– subdir	Untergeordnete Verzeichnisse prüfen (Standardeinstellung)
– no-subdir	Untergeordnete Verzeichnisse nicht prüfen
– max-subdir-level = LEVEL	Maximale Verschachtelungsebene (LEVEL) bei untergeordneten Verzeichnissen (Standardeinstellung: 0 = unbegrenzt)
– symlink	Symbolischen Verknüpfungen folgen (Standardeinstellung)
– no-symlink	Symbolische Verknüpfungen übergehen
– ext-remove = EXTENSIONS	
– ext-exclude = EXTENSIONS	Angegebene EXTENSIONS von der Prüfung ausschließen (durch einen Doppelpunkt voneinander getrennt)

Methoden:

– adware	Auf Adware/Spyware/Riskware prüfen
– no-adware	Nicht auf Adware/Spyware/Riskware prüfen
– unsafe	Auf potenziell unsichere Anwendungen prüfen
– no-unsafe	Nicht auf potenziell unsichere Anwendungen prüfen
– unwanted	Auf potenziell unerwünschte Anwendungen prüfen
– no-unwanted	Nicht auf potenziell unerwünschte Anwendungen prüfen
– pattern	Signaturen verwenden
– no-pattern	Signaturen nicht verwenden
– heur	Heuristik aktivieren
– no-heur	Heuristik deaktivieren
– adv-heur	Erweiterte Heuristik aktivieren
– no-adv-heur	Erweiterte Heuristik deaktivieren

Schadcode entfernen:

– action = ACTION	Aktion ACTION für infizierte Objekte ausführen Mögliche Aktionen: none, clean, prompt (keine, Schadcode entfernen, Aufforderung anzeigen)
– quarantine	Infizierte Dateien in Quarantäneordner kopieren (ergänzt ACTION)
– no-quarantine	Infizierte Dateien nicht in Quarantäneordner kopieren

Logs:

– log-file=FILE	Ausgabe in Datei FILE aufzeichnen
– log-rewrite	Ausgabedatei überschreiben (Standardeinstellung: append (anhängen))
– log-all	Nicht-Infizierte Dateien ebenfalls ins Log aufnehmen
– no-log-all	Nicht-Infizierte Dateien nicht ins Log aufnehmen (Standardeinstellung)

Mögliche Exit-Codes der Prüfung:

0 – Keine Bedrohung gefunden
1 – Bedrohung gefunden, aber nicht entfernt
10 – Noch mehrere infizierte Dateien vorhanden
101 – Archivierungsfehler
102 – Zugriffsfehler
103 – Interner Fehler

HINWEIS: Exit-Codes über 100 bedeuten, dass die Datei nicht geprüft wurde und daher infiziert sein kann.

5.4 ESET SysInspector

ESET SysInspector ist eine Anwendung, die Ihren Computer gründlich prüft und erfasste Daten umfassend anzeigt. Informationen wie installierte Treiber und Anwendungen, Netzwerkverbindungen oder wichtige Einträge in der Registrierung können für Sie nützlich sein, wenn Sie ein verdächtiges Systemverhalten prüfen, ob dieses nun auf einer Software- oder Hardwareinkompatibilität oder auf einer Infektion mit Schadsoftware beruht.

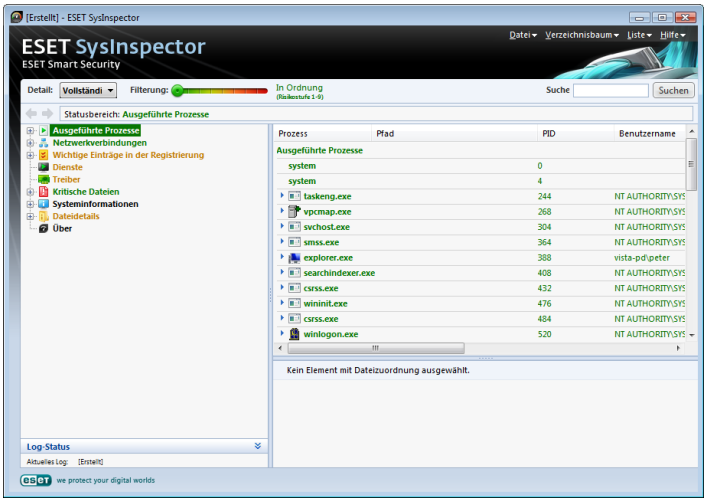
ESET bietet SysInspector in zwei Varianten an. Die Portable-Anwendung (SysInspector.exe) kann über die ESET-Website kostenlos heruntergeladen werden. Die integrierte Variante ist in ESET Smart Security 4 enthalten. Um den SysInspector-Abschnitt zu öffnen, aktivieren Sie in der Ecke links unten den Modus für die erweiterte Anzeige und klicken Sie auf **Tools > SysInspector**. Beide Varianten verfügen über identische Funktionen sowie über dieselben Programmsteuerungen. Der einzige Unterschied liegt in der Art, wie die Ausgaben verwaltet werden. Mit der Portable-Anwendung können Sie einen Systemsnapshot als XML-Datei exportieren und auf Ihrem Laufwerk speichern. Dies ist auch bei der integrierten Version von SysInspector möglich. Außerdem können Sie Ihre Systemsnapshots einfach direkt unter **ESET Smart Security 4 > Tools > SysInspector** speichern (weitere Informationen unter 5.4.1.4 SysInspector als Teil von ESS).

Gedulden Sie sich einen Moment, während ESET SysInspector Ihren Computer prüft. Es kann zwischen 10 Sekunden und einigen Minuten dauern, je nach Hardware-Konfiguration, Betriebssystem und Zahl der auf dem Computer installierten Anwendungen.

5.4.1 Verwendung von Benutzeroberfläche und Anwendung

Aus Gründen der Benutzerfreundlichkeit ist das Hauptfenster in vier Abschnitte unterteilt – Oben im Hauptfenster befindet sich

die Programmsteuerung, links das Navigationsfenster, rechts in der Mitte das Beschreibungsfenster und rechts unten im Hauptfenster das Detailfenster.



5.4.1.1 Programmsteuerung

Dieser Abschnitt enthält die Beschreibung aller Programmsteuerungen, die in ESET SysInspector verfügbar sind.

Datei
Indem Sie hier klicken, können Sie Ihren aktuellen Berichtsstatus zur späteren Prüfung speichern oder einen zuvor gespeicherten Bericht öffnen. Wenn Sie Ihren Bericht veröffentlichen möchten, empfehlen wir, diesen " in zum Senden geeigneter Form zu generieren. In dieser Form sind im Bericht keine vertraulichen Informationen enthalten.

Hinweis: *Sie können zuvor gespeicherte ESET SysInspector-Berichte öffnen, indem Sie diese einfach per Drag-and-Drop in das Hauptfenster verschieben.*

Verzeichnisbaum
Ermöglicht Ihnen das Erweitern oder Schließen sämtlicher Knoten

Liste
Enthält Funktionen zur leichteren Navigation innerhalb des Programms sowie verschiedene andere Funktionen, etwa für die Online-Informationssuche.

Wichtig: *Rot hervorgehobene Elemente sind unbekannt. Deshalb werden Sie vom Programm als potenziell gefährlich gekennzeichnet. Wenn ein Element rot markiert ist, bedeutet dies nicht automatisch, dass Sie die Datei löschen können. Vergewissern Sie sich vor dem Löschen, dass die Dateien wirklich gefährlich oder unnötig sind.*

Hilfe
Enthält Informationen zur Anwendung und zu ihren Funktionen.

Detail
Beeinflusst Informationen, die in anderen Abschnitten des Hauptfensters angezeigt werden, wodurch sich die Verwendung des Programms einfach gestaltet. Im Modus *Einfach* haben Sie Zugriff auf Informationen, die Sie zur Suche nach Lösungen für häufig auftretende Systemprobleme verwenden können. Im Modus *Mittel* werden im Programm die weniger genutzten Details angezeigt, während ESET SysInspector im Modus *Vollständig* sämtliche Informationen anzeigt, die zur Lösung sehr spezifischer Probleme erforderlich sind.

Filterung der Elemente
Am besten wird die Filterung der Elemente genutzt, um verdächtige Dateien oder Einträge in der Registrierung Ihres Systems zu suchen. Indem Sie den Schieber anpassen, können Sie Elemente nach ihrer Risikostufe filtern. Wenn sich der Schieber ganz links befindet (Risikostufe 1), werden alle Elemente angezeigt. Wenn Sie den Schieber nach rechts bewegen, filtert das Programm alle Elemente heraus, die unterhalb der aktuellen Risikostufe liegen. Es werden nur Elemente angezeigt, die verdächtiger sind als die angezeigte Stufe. Wenn sich der Schieber ganz rechts befindet, werden nur bekannte schädliche

Elemente durch das Programm angezeigt.

Alle Elemente, die in den Risikobereich 6 bis 9 gehören, können ein Sicherheitsrisiko darstellen. Wenn Sie keine der Sicherheitslösungen von ESET verwenden, empfehlen wir, dass Sie Ihr System mit ESET Online Scanner prüfen, wenn das Programm solch ein Element gefunden hat. ESET Online Scanner ist ein kostenloser Dienst und ist unter http://www.eset.eu/online-scanner verfügbar.

Hinweis: *Die Risikostufe eines Elements kann schnell ermittelt werden, indem die Farbe des Elements mit der Farbe auf dem Schieber für die Risikostufe verglichen wird.*

SucheS
Die Suche kann verwendet werden, um ein bestimmtes Element schnell nach seinem Namen oder nach einem Teil des Namens zu suchen. Die Ergebnisse der Suchanfrage werden im Beschreibungsfenster angezeigt.

Zurück
Indem Sie auf den Zurück- oder Vorwärtspfeil klicken, können Sie zu vorher angezeigten Informationen im Beschreibungsfenster zurückkehren.

Statusbereich
Zeigt den aktuellen Knoten im Navigationsfenster an.

5.4.1.2 Navigation in ESET SysInspector

In ESET SysInspector werden verschiedene Informationsarten in mehrere grundlegende Abschnitte unterteilt, die als Knoten bezeichnet werden. Falls verfügbar können Sie zusätzliche Details finden, indem Sie die einzelnen Knoten um ihre Unterknoten erweitern. Um einen Knoten zu öffnen oder zu verkleinern, doppelklicken Sie einfach auf den Namen des Knotens oder klicken Sie neben dem Knotennamen auf ⊞ oder auf ⊟. Wenn Sie den Verzeichnisbaum der Knoten und Unterknoten im Navigationsfenster durchsuchen, können Sie verschiedene Details zu den einzelnen Knoten finden, die im Beschreibungsfenster angezeigt werden. Wenn Sie die Elemente im Beschreibungsfenster durchsuchen, werden gegebenenfalls weitere Details zu den einzelnen Elementen im Detailfenster angezeigt.

Im Folgenden werden die Hauptknoten des Navigationsfensters beschrieben sowie die dazugehörigen Informationen im Beschreibungs- und Detailfenster.

Laufende Prozesse
Dieser Knoten enthält Informationen über Anwendungen und Prozesse, die zum Zeitpunkt der Berichterstellung ausgeführt werden. Im Beschreibungsfenster können Sie zusätzliche Details zu den einzelnen Prozessen finden, etwa von dem Prozess genutzte dynamische Bibliotheken und deren Ort im System, den Namen des Anwendungsanbieters, die Risikostufe der Datei usw.

Das Detailfenster enthält zusätzliche Informationen zu Elementen, die im Beschreibungsfenster ausgewählt werden, etwa die Größe der Datei oder ihr Hash-Wert.

Hinweis: *Ein Betriebssystem enthält mehrere wichtige Kernkomponenten, die rund um die Uhr ausgeführt werden und grundlegende kritische Funktionen für andere Benutzeranwendungen bereitstellen. In bestimmten Fällen werden solche Prozesse im Tool ESET SysInspector mit einem Dateipfad angezeigt, der mit \??\ beginnt. Diese Symbole bieten eine Optimierung für diese Prozesse vor dem Start. Sie sind für das System sicher und dementsprechend korrekt.*

Netzwerkverbindungen
Das Beschreibungsfenster enthält eine Liste mit Prozessen und Anwendungen, die über das Netzwerk kommunizieren und dabei das Protokoll verwenden, das im Navigationsfenster (TCP oder UDP) ausgewählt wurde, zusammen mit der Remote-Adresse, mit der die Anwendung verbunden ist. Sie können auch IP-Adressen prüfen, die über eine DNS-Zuweisung zugewiesen wurden.

Das Detailfenster enthält zusätzliche Informationen zu Elementen, die im Beschreibungsfenster ausgewählt werden, etwa die Größe der Datei oder ihr Hash-Wert.

Wichtige Einträge in der Registrierung
Enthält eine Liste von ausgewählten Einträgen in der Registrierung, die häufig mit verschiedenen Systemproblemen in Verbindung stehen, etwa im Hinblick auf die Festlegung von Systemstartprogrammen, Browser Helper Objects (BHO) usw.

Im Beschreibungsfenster wird angezeigt, welche Dateien mit bestimmten Einträgen in der Registrierung verbunden sind. Gegebenenfalls werden zusätzliche Details im Detailfenster angezeigt.

Dienste
Das Beschreibungsfenster enthält eine Liste von Dateien, die als Windows-Dienste registriert sind. Im Detailfenster können Sie die Einstellung für den Start des Dienstes prüfen sowie bestimmte Details in Zusammenhang mit der Datei.

Treiber
Eine Liste der Treiber, die auf dem System installiert sind.

Kritische Dateien
Im Beschreibungsfenster werden Inhalte von kritischen Dateien angezeigt, die mit dem Microsoft Windows Betriebssystem in Zusammenhang stehen.

Systeminformationen
Enthält detaillierte Informationen zur Hard- und Software sowie Informationen über die eingestellten Umgebungsvariablen und Benutzerrechte.

Dateidetails
Eine Liste wichtiger Systemdateien und Dateien im Ordner der Programmdateien. Zusätzliche Informationen bezüglich der Dateien können dem Beschreibungsfenster und dem Detailfenster entnommen werden.

Über
Informationen über ESET SysInspector

5.4.1.3 Vergleichen

Die Vergleichsfunktion ermöglicht dem Benutzer, zwei vorhandene Log-Dateien zu vergleichen. Das Ergebnis dieser Funktion besteht aus einem Satz von Elementen, in denen sich beide Log-Dateien unterscheiden. Die Funktion ist geeignet, wenn Sie Veränderungen im System verfolgen möchten. Sie können beispielsweise die Aktivität von Schadcode erkennen.

Nach dem Start erstellt die Anwendung eine neue Log-Datei, die in einem neuen Fenster angezeigt wird. Wählen Sie die Option **Datei** -> **Log speichern** aus, um eine Log-Datei zu speichern. Log-Dateien können später geöffnet und angezeigt werden. Um eine bestehende Log-Datei zu öffnen, wählen Sie im Menü **Datei** -> **Log öffnen**. Im Hauptfenster des Programms wird in ESET SysInspector stets eine einzelne Log-Datei angezeigt.

Bei einem Vergleich von zwei Log-Dateien wird eine gegenwärtig aktive Log-Datei mit einer gespeicherten Log-Datei verglichen. Um Log-Dateien zu vergleichen, verwenden Sie die Option **Datei** -> **Logs vergleichen** und wählen Sie **Datei auswählen**. Die ausgewählte Log-Datei wird mit der aktiven Datei aus dem Hauptprogrammfenster verglichen. In der sich daraus ergebenden Vergleichs-Log-Datei werden nur die Unterschiede zwischen den beiden Log-Dateien aufgeführt.

Hinweis: *Wenn Sie zwei Log-Dateien vergleichen, die Optionen Datei -> Log speichern auswählen und die Datei als ZIP-Datei speichern, werden beide Dateien gespeichert. Wenn Sie eine derartige Datei später öffnen, werden die enthaltenen Log-Dateien automatisch verglichen.*

Neben den angezeigten Elementen weden in SysInspector Symbole dargestellt, die Unterschiede zwischen den verglichenen Log-Dateien erfassen. Elemente, die mit ➖ gekennzeichnet sind, sind nur in der aktiven Log-Datei enthalten, nicht jedoch in der geöffneten Vergleichs-Log-Datei. Elemente, die dagegen mit ➕ gekennzeichnet sind, waren nur in der geöffneten Log-Datei enthalten und fehlen in der aktiven Log-Datei.

Beschreibung aller Symbole, die neben Elementen angezeigt werden können:

➕ neuer Wert, nicht in der vorherigen Log-Datei enthalten

Abschnitt der Baumstruktur enthält neue Werte

➖ entfernter Wert, nur in der vorherigen Log-Datei enthalten

Abschnitt der Baumstruktur enthält entfernte Werte

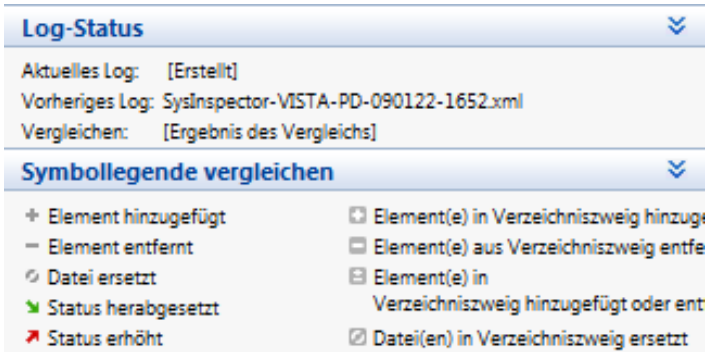
Wert / Datei wurde geändert

Abschnitt der Baumstruktur enthält geänderte Werte / Dateien

die Risikostufe ist gesunken / war in der vorherigen Log-Datei höher

die Risikostufe ist gestiegen / war in der vorherigen Log-Datei niedriger

In den Erklärungen, die unten links angezeigt werden, werden alle Symbole erläutert. Außerdem werden dort die Namen der Log-Dateien angezeigt, die miteinander verglichen werden.



Jede Vergleichs-Log-Datei kann als Datei gespeichert und später geöffnet werden.

Beispiel:
Generieren und speichern Sie eine Log-Datei, in der die ursprünglichen Informationen über das System aufgezeichnet werden, als Datei mit dem Namen „zuvor.xml". Nachdem Veränderungen am System vorgenommen wurden, öffnen Sie SysInspector und lassen Sie das Programm eine neue Log-Datei erstellen. Speichern Sie diese als Datei unter dem Namen „aktuell.xml".

Um Veränderungen zwischen diesen beiden Log-Dateien nachzuverfolgen, wählen Sie die Optionen **Datei** -> **Logs vergleichen** aus. Das Programm erstellt eine Vergleichs-Log-Datei, in der die Unterschiede zwischen den beiden Log-Dateien angezeigt werden.

Zum selben Ergebnis gelangen Sie, wenn Sie die folgende Befehlszeilenoption verwenden:

SysIsnpector.exe aktuell.xml zuvor.xml

5.4.1.4 SysInspector als Bestandteil von ESET Smart Security 4

Um den SysInspector-Bereich in ESET Smart Security 4 zu öffnen, klicken Sie auf **Tools** > **SysInspector**. Das Verwaltungssystem im SysInspector-Fenster ähnelt dem von Prüfungslogs oder geplanten Tasks. Alle Vorgänge mit Systemsnapshots - Erstellen, Anzeigen, Vergleichen, Entfernen und Exportieren - sind mit einem oder zwei Klicks zugänglich.

Das SysInspector-Fenster enthält Basisinformationen zum erstellten Snapshot wie z. B. Erstellungszeitpunkt, kurzer Kommentar, Name des Benutzers, der den Snapshot erstellt hat sowie den Status des Snapshots.

Verwenden Sie zum **Vergleichen, Hinzufügen...** oder **Entfernen** von Snapshots die entsprechenden Schaltflächen unterhalb der Snapshotliste im SysInspector-Fenster. Diese Optionen sind ebenfalls im Kontextmenü verfügbar. Um den gewählten Systemsnapshot anzuzeigen, verwenden Sie die Option **Anzeigen** im Kontextmenü. Um den gewünschten Snapshot in eine Datei zu exportieren, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Exportieren...**. Im Folgenden eine kurze Beschreibung der verfügbaren Optionen:

Vergleichen – ermöglicht den Vergleich zweier vorhandener Logs. Diese Option ist dazu geeignet, Änderungen zwischen dem aktuellen und einem älteren Log nachzuvollziehen. Hierfür müssen Sie zwei Snapshots für den Vergleich auswählen.

Hinzufügen – fügt einen neuen Eintrag hinzu. Zuvor müssen Sie einen kurzen Kommentar zum Eintrag eingeben. In der Spalte Status wird der Status der Erstellung des aktuellen Snapshots in Prozent angezeigt. Alle fertiggestellten Snapshots sind mit dem Status Erstellt markiert.

Entfernen – Entfernen von Einträgen aus der Liste

Anzeigen – den ausgewählten Snapshot anzeigen. Sie können auch auf den ausgewählten Eintrag doppelklicken.

Exportieren... – speichert den ausgewählten Eintrag in einer XML-Datei (auch in einer komprimierten Version).

5.4.1.5 Dienste-Skript

Das Dienste-Skript ist ein Hilfsmittel, das sich direkt auf das Betriebssystem und die installierten Anwendungen auswirkt. Damit können Benutzer Skripte ausführen, die problematische Komponenten wie Viren, Überreste von Viren, blockierte Dateien, Vireneinträge in der Registrierung usw. aus dem System entfernen. Das Skript wird in einer Textdatei gespeichert, die aus einer vorhandenen XML-Datei erstellt ist. Die Daten in der TXT-Skriptdatei sind für die einfache Verwendung einfach und verständlich angeordnet. Das Skript verhält sich zunächst neutral. In seiner ursprünglichen Form zeigt es keinerlei Wirkung auf das System. Der Benutzer muss das Skript verändern, bevor es aktiv wird.

Warnung:
Dieses Hilfsmittel sollte nur von erfahrenen Benutzern eingesetzt werden. Die unsachgemäße Anwendung kann zu Schäden an Programmen oder dem Betriebssystem führen.

5.4.1.5.1 Dienste-Skripten erstellen

Zum Erzeugen eines Skripts klicken Sie mit der rechten Maustaste auf ein beliebiges Element der Baumstruktur des Menüs (im linken Bereich) des Hauptfensters von SysInspector. Wählen Sie aus dem Kontextmenü entweder die Option **„Alle Bereiche in das Dienste-Skript exportieren"** oder die Option **„Ausgewählte Bereiche in das Dienste-Skript exportieren"**.

5.4.1.5.2 Struktur des Dienste-Skripts

In der ersten Zeile des Dateikopfs des Skripts finden Sie Informationen zur Version der Engine (ev), der Version der Benutzeroberfläche (gv) und der Log-Version (lv). Anhand dieser Daten können Sie mögliche Änderungen an der XML-Datei, die das Skript erzeugt, sowie Inkonsistenzen bei der Ausführung aufspüren. Dieser Teil des Skripts sollte nicht geändert werden.

Die übrige Datei ist in zwei Abschnitte unterteilt, deren Elemente bearbeitet werden können (und vom Skript verarbeitet werden). Sie können Elemente für die Verarbeitung markieren, indem Sie das

„-"-Zeichen vor einem Element durch ein „+"-Zeichen ersetzen. Die einzelnen Abschnitte des Skripts werden durch eine Leerzeile voneinander getrennt. Jeder Abschnitt verfügt über eine Nummer und einen Titel.

01) Ausgeführte Prozesse

Dieser Abschnitt enthält eine Liste aller auf dem System ausgeführten Prozesse. Jeder Prozess ist durch seinen UNC-Pfad sowie seinen CRC 16-Hash-Code in Sternchen (*) gekennzeichnet.

Beispiel:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In diesem Beispiel wurde der Prozess module32.exe ausgewählt (mit einem „+"-Zeichen markiert) und wird nach Ausführung des Skripts beendet.

02) Geladene Module

Dieser Abschnitt führt die derzeit verwendeten Systemmodule auf.

Beispiel:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In diesem Beispiel wurde das Modul khbekhb.dll mit einem „+"-Zeichen gekennzeichnet. Wenn das Skript ausgeführt wird, erkennt es die Prozesse, die dieses bestimmte Modul verwenden, und beendet diese.

03) TCP connections (TCP-Verbindungen)

Dieser Abschnitt enthält Informationen über bestehende TCP-Verbindungen.

Beispiel:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 ->
127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 ->
127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 ->
127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe
Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Bei Ausführung des Skripts wird der Besitzer des Sockets der markierten TCP-Verbindungen ermittelt. Die Socket-Verbindung wird beendet, wodurch Systemressourcen freigegeben werden.

04) UDP-Endpunkte

Dieser Abschnitt enthält Informationen über bestehende UDP-Endpunkte.

Beispiel:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Bei Ausführung dieses Skripts wird der Besitzer des Sockets der markierten UDP-Endpunkte ermittelt und die Socket-Verbindung beendet.

05) DNS-Server-Einträge

Dieser Abschnitt enthält Informationen über die aktuelle DNS-Server-Konfiguration.

Beispiel:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Die markierten DNS-Servereinträge werden bei Ausführung des Skripts entfernt.

06) Wichtige Registrierungseinträge

Dieser Abschnitt enthält Informationen über wichtige Registrierungseinträge.

Beispiel:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\
Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Die markierten Einträge werden bei Ausführung des Skripts gelöscht, auf 0 Byte-Werte reduziert oder auf ihre Standardwerte gesetzt. Die jeweilige Aktion für die einzelnen Einträge hängt von der Kategorie des Eintrags und vom Schlüsselwert in der jeweiligen Registrierung ab.

07) Dienste

Dieser Abschnitt führt die im System registrierten Dienste auf.

Beispiel:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\
windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\
windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path:
c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

Die markierten Dienste und die davon abhängigen Dienste werden bei Ausführung des Skripts abgebrochen und deinstalliert.

08) Treiber

Dieser Abschnitt führt die installierten Treiber auf.

Beispiel:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\
system32\drivers\acpi.sys, state: Running, startup:
Boot
- Name: ADI UAA Function Driver for High Definition
Audio Service, exe path: c:\windows\system32\drivers\
adihdaud.sys, state: Running, startup: Manual
[...]
```

Wenn Sie das Skript ausführen, werden die ausgewählten Treiber aus der Registrierung und dem System entfernt.

09) Kritische Dateien

Dieser Abschnitt enthält Informationen über Dateien, die für das fehlerfreie Funktionieren des Betriebssystems maßgeblich sind.

Beispiel:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[…]

* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[…]

* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[…]
```

Die ausgewählten Elemente werden entweder gelöscht oder auf ihre ursprünglichen Werte zurückgesetzt.

5.4.1.5.3 Dienste-Skripten ausführen

Markieren Sie alle gewünschten Elemente. Speichern und schließen Sie dann das Skript. Führen Sie das Skript direkt im Hauptfenster von SysInspector aus, indem Sie im Menü „Datei" die Option **„Dienste-Skript ausführen"** wählen. Wenn Sie ein Skript öffnen, wird folgende Meldung angezeigt: **„Möchten Sie das Dienste-Skript "%s" wirklich ausführen?"** Wenn Sie Ihre Auswahl bestätigen, wird unter Umständen eine weitere Warnung mit dem Hinweis angezeigt, dass das gewünschte Dienste-Skript nicht signiert ist. Klicken Sie auf **„Ausführen"**, um das Skript zu starten.

Daraufhin wird in einem Dialogfenster angezeigt, dass das Skript erfolgreich ausgeführt wurde.

Sollte das Skript nur teilweise ausgeführt worden sein, wird ein Dialogfenster mit der folgenden Meldung angezeigt: **„Das Dienste-Skript wurde teilweise ausgeführt. Möchten Sie den Fehlerbericht anzeigen?"** Wählen Sie **„Ja"**, um einen umfangreichen Fehlerbericht mit den nicht ausgeführten Vorgängen anzuzeigen.

Wenn Ihr Skript nicht erkannt und nicht ausgeführt wurde, erhalten Sie die folgende Meldung: **„Bestehen Konsistenzprobleme mit dem Skript (beschädigter Dateikopf, fehlerhafte Abschnittstitel, fehlende Leerzeilen zwischen den Abschnitten etc.)?"** In diesem Fall öffnen Sie entweder die Skriptdatei neu und beheben die Fehler, oder Sie erstellen ein neues Dienste-Skript.

5.5 ESET SysRescue

Bei ESET Recovery CD (ERCD) handelt es sich um ein Dienstprogramm, das ein bootfähiges Medium mit ESET Smart Security 4 (ESS) erstellt. Der große Vorteil von ESET Recovery CD ist, dass ESS unabhängig vom Host-Betriebssystem laufen kann, gleichzeitig jedoch vollen Zugriff auf Laufwerke und Dateisystem hat. Dies bietet die Möglichkeit, die eingedrungene Schadsoftware zu entfernen, die normalerweise nicht gelöscht werden kann (z. B. während das Betriebssystem läuft usw.).

5.5.1 Minimalanforderungen

ESET SysRescue (ESR) läuft in der Umgebung Microsoft Windows Preinstallation Environment (Windows PE) Version 2.x, die auf Windows Vista basiert. Windows PE ist Teil des kostenlosen Windows Automated Installation Kit (Windows AIK). Aus diesem Grund muss AIK vor dem Erstellen von ESR installiert werden. Da die 32-Bit-Version von Windows PE unterstützt wird, kann ESR nur in der 32-Bit-Version von ESS/ENA erstellt werden. ESR unterstützt Windows AIK 1.1 und höher. ESR ist in ESS/ENA 4.0 und höher verfügbar.

5.5.2 So erstellen Sie eine Rettungs-CD

Wenn die Minimalanforderungen für die Erstellung der ESET SysRescue (ESR)-CD erfüllt sind, sollte es keine Probleme geben. Klicken Sie auf **Start** > **Programme** > **ESET** > **ESET Smart Security 4** > **ESET SysRescue**, um den ESR-Assistenten zu starten.

Zuerst prüft der Assistent, ob Windows AIK und ein geeignetes Gerät für die Erstellung von Bootmedien verfügbar sind.

Als nächstes müssen Sie das Zielmedium für das ESR auswählen. Neben CD/DVD/USB können Sie das ESR auch in einer ISO-Datei speichern. Später können Sie dann das ISO-Bild auf CD/DVD brennen oder es anderweitig verwenden (z. B. in einer virtuellen Umgebung wie VmWare oder Virtualbox).

Nachdem Sie alle Einstellungen vorgenommen haben, sehen Sie im letzten Schritt des ESET SysRescue-Assistenten eine Kompilationsvorschau. Prüfen Sie die Einstellungen und starten Sie die Kompilation. Folgende Optionen stehen zur Verfügung:

Ordner
ESET Antivirus
Erweitert
Bootfähiges USB-Gerät
Brennen

5.5.2.1 Ordner

Temporärer Ordner ist ein Arbeitsverzeichnis für Dateien, die während der ESET SysRescue-Kompilation erforderlich sind.

ISO-Ordner ist ein Ordner, in dem die resultierende ISO-Datei nach Abschluss der Kompilation gespeichert wird.

In der Liste auf dieser Registerkarte werden alle lokalen und verbundenen Netzlaufwerke zusammen mit dem verfügbaren freien Speicherplatz angezeigt. Wenn sich einige der Ordner auf einem Laufwerk mit zu wenig Speicherplatz befinden, empfehlen wir, dass Sie ein anderes Laufwerk mit mehr freiem Speicherplatz auswählen. Andernfalls wird die Kompilation möglicherweise verfrüht abgebrochen, weil zu wenig freier Speicherplatz auf dem Laufwerk zur Verfügung steht.

Externe Anwendungen
Erlaubt es Ihnen, weitere Programme festzulegen, die nach dem Bootvorgang über ein SysRescue-Medium ausgeführt oder installiert werden.

Externe Anwendungen einbeziehen – ermöglicht das Hinzufügen externer Programme zur SysRescue-Kompilation

Ausgewählter Ordner – Ordner, in dem sich die Programme befinden, die zum SysRescue-Laufwerk hinzugefügt werden sollen

5.5.2.2 ESET Antivirus

Zum Erstellen der ESET SysRescue-CD können Sie zwei Quellen von ESET-Dateien auswählen, die vom Compiler verwendet werden sollen.

ESS-Ordner – Dateien, die bereits im Ordner enthalten sind, in dem das ESET-Produkt auf dem Computer installiert ist

MSI-Datei – Dateien, die im MSI-Installationsprogramm enthalten sind, werden verwendet

Profil – Sie können eine der folgenden beiden Quellen für Benutzername und Passwort verwenden:

Installiertes ESS – Benutzername und Passwort werden von der gegenwärtig installierten Version von ESET Smart Security 4 bzw. ESET NOD32 kopiert

Von Benutzer – Es werden Benutzername und Passwort verwendet, die in den entsprechenden Textfeldern unten eingegeben wurden

Hinweis: *ESET Smart Security 4 oder ESET NOD32 Antivirus auf der ESET SysRescue-CD werden entweder über das Internet oder über die ESET Security-Lösung aktualisiert, die auf dem Computer installiert ist, auf dem die ESET SysRescue-CD ausgeführt wird.*

5.5.2.3 Erweitert

Über die Registerkarte **Erweitert** können Sie die ESET-SysRescue-CD für die Größe des Speichers Ihres Computers optimieren. Wählen Sie **512 MB und mehr** , um den Inhalt der CD in den Arbeitsspeicher (RAM) zu schreiben. Wenn Sie **weniger als 512 MB** auswählen, wird permanent auf die Recovery-CD zugegriffen, wenn WinPE ausgeführt wird.

Externe Treiber – In diesem Abschnitt können Sie Treiber für Ihre spezielle Hardware (normalerweise Netzwerkadapter) einfügen. Auch wenn WinPE auf Windows Vista SP1 basiert, von dem eine große Hardwarepalette unterstützt wird, wird Hardware bisweilen nicht erkannt und Sie müssen den Treiber manuell hinzufügen. Es gibt zwei Methoden, um den Treiber zur ESET SysRescue-Kompilation hinzuzufügen – manuell (die Schaltfläche **Hinzufügen**) und automatisch (die Schaltfläche **Autom. Suche**). Im Fall des manuellen Hinzufügens müssen Sie den Pfad zur entsprechenden .inf-Datei auswählen (die entsprechende *.sys-Datei muss ebenfalls in diesem Ordner enthalten sein). Wenn Sie den Treiber automatisch hinzufügen, wird dieser automatisch im Betriebssystem des betreffenden Computers gesucht. Wir empfehlen, das automatische Hinzufügen nur zu nutzen, wenn SysRescue auf einem Computer mit demselben Netzwerkadapter verwendet wird wie der, der bei dem Computer verwendet wird, auf dem SysRescue erstellt wird. Während der Erstellung von ESET SysRescue wird der Treiber zur Kompilation hinzugefügt, sodass der Benutzer später nicht separat danach suchen muss.

5.5.2.4 Bootfähiges USB-Gerät

Wenn Sie ein USB-Gerät als Zielmedium ausgewählt haben, können Sie eines der verfügbaren USB-Medien auf der Registerkarte für die bootfähigen USB-Geräte (falls mehrere USB-Geräte verfügbar sind) auswählen.

Warnung: *Das ausgewählte USB-Gerät wird während des Prozesses der ESET SysRescue-Erstellung formatiert, was bedeutet, dass alle Daten auf dem Gerät gelöscht werden.*

5.5.2.5 Brennen

Wenn Sie CD/DVD als Zielmedium ausgewählt haben, können Sie weitere Parameter für das Brennen auf der Registerkarte für das Brennen festlegen.

ISO-Datei löschen – aktivieren Sie diese Option, um die ISO-Dateien zu löschen, nachdem die ESET Rescue-CD erstellt wurde.

Löschen aktiviert – Sie können das schnelle Löschen und das vollständige Löschen auswählen.

Brennerlaufwerk – Wählen Sie das Laufwerk zum Brennen aus.

Warnung: *Dies ist die standardmäßige Option. Wenn eine wiederbeschreibbare CD/DVD verwendet wird, werden alle darauf enthaltenen Daten gelöscht.*

Der Abschnitt zu den Medien enthält Informationen zu dem Medium, das gegenwärtig in Ihr CD/DVD-Laufwerk eingelegt ist.

Schreibgeschwindigkeit–Wählen Sie die gewünschte Geschwindigkeit im Dropdown-Menü aus. Die Möglichkeiten Ihres Brennerlaufwerks und der verwendete CD/DVD-Typ sollten bei der Auswahl der Schreibgeschwindigkeit berücksichtigt werden.

5.5.3 Arbeiten mit ESET SysRescue

Zur effizienten Nutzung der Rettungs-CD/DVD bzw. des Rettungs-USB-Mediums muss der Computer vom ESET SysRescue-Bootmedium aus gestartet werden. Die Bootpriorität kann im BIOS geändert werden. Alternativ können Sie während des Computerstarts auch das Bootmenü aufrufen. Hierzu wird abhängig von Ihrer Motherboard/BIOS-Variante üblicherweise eine der Tasten F9-F12 verwendet.

Nach dem Hochfahren starten ESS/ENA. Da ESET SysRescue nur in bestimmten Situationen verwendet wird, sind manche Schutzmodule und Programmfunktionen nicht erforderlich, die bei ESS/ENA normalerweise fester Bestandteil sind. Die Liste wird auf „Prüfung des Computers", „Update" und einige Bereiche in „Einstellungen" begrenzt. Die wichtigste Funktion von ESET SysRescue ist die Möglichkeit, die Signaturdatenbank zu aktualisieren. Wir empfehlen, vor dem Start der Computerprüfung ein Update des Programms durchzuführen.

5.5.3.1 ESET SysRescue verwenden

Nehmen wir an, dass Computer im Netzwerk mit einem Virus infiziert wurden, der ausführbare Dateien (EXE) verändert. Mit ESS/ENA können Sie alle infizierten Dateien bereinigen. Einzige Ausnahme ist die Datei explorer.exe, die selbst im abgesicherten Modus nicht bereinigt werden kann.

Dies liegt daran, dass explorer.exe, als einer der grundlegenden Windows-Prozesse, auch im abgesicherten Modus gestartet wird. ESS/ENA kann mit der Datei keine Aktionen ausführen, und deshalb bleibt sie infiziert.

In diesem Fall können Sie das Problem mit ESET SysRescue lösen. ESET SysRescue benötigt keine Komponenten des Host-Betriebssystems. Deshalb kann es alle Dateien der Festplatte verarbeiten (bereinigen, löschen).

6. Glossar

6.1 Schadsoftwaretypen

Bei Schadsoftware handelt es sich um bösartige Software, die in einen Computer eindringt und/oder auf einem Computer Schaden anrichtet.

6.1.1 Viren

Bei einem Computervirus handelt es sich um eingedrungene Schadsoftware, die auf Ihrem Computer befindliche Dateien beschädigt. Ihren Namen haben sie nicht umsonst mit den Viren aus der Biologie gemein. Schließlich verwenden sie ähnliche Techniken, um sich vom einen zum anderen Computer auszubreiten.

Computerviren greifen hauptsächlich ausführbare Dateien und Dokumente an. Um sich zu vermehren, hängt sich ein Virus mit seinem „Körper" an das Ende einer Zieldatei an. Und so funktioniert ein Computervirus: Durch Ausführung der infizierten Datei wird der Virus aktiviert (noch bevor die eigentliche Anwendung gestartet wird) und führt seinen vordefinierten Task aus. Erst dann wird die eigentliche Anwendung gestartet. Ein Virus kann einen Computer also nur dann infizieren, wenn der Benutzer selbst (versehentlich oder absichtlich) das bösartige Programm ausführt oder öffnet.

Computerviren unterscheiden sich durch Art und Schweregrad der durch sie verursachten Schäden. Einige von ihnen sind aufgrund ihrer Fähigkeit, Dateien von der Festplatte gezielt zu löschen, äußerst gefährlich. Andererseits gibt es aber auch Viren, die keinen wirklichen Schaden verursachen–ihr einziger Zweck besteht darin, den Benutzer zu verärgern und die technischen Fähigkeiten ihrer Urheber unter Beweis zu stellen.

Es soll an dieser Stelle jedoch darauf hingewiesen werden, dass Viren (verglichen mit Trojanern oder Spyware) allmählich immer mehr zur Seltenheit werden, da sie für Urheber von bösartiger Software aus kommerzieller Sicht nicht attraktiv sind. Außerdem wird der Begriff „Virus" oft fälschlicherweise für alle Arten von Schadsoftware verwendet. Gegenwärtig setzt sich nach und nach der neue, zutreffendere Begriff „Malware" (bösartige Software) durch.

Wenn Ihr Computer von einem Virus infiziert wurde, ist es notwendig, den Originalzustand der infizierten Dateien wiederherzustellen–das heißt, den Schadcode mithilfe eines Virenschutzprogrammes daraus zu entfernen.

Viren sind beispielsweise: OneHalf, Tenga und Yankee Doodle.

6.1.2 Würmer

Bei einem Computerwurm handelt es sich um ein Programm, das einen bösartigen Code enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Der grundlegende Unterschied zwischen Viren und Würmern besteht darin, dass Würmer in der Lage sind, sich selbstständig zu vermehren und zu verbreiten. Das heißt, sie sind unabhängig von Wirtsdateien (oder Bootsektoren).

Würmer verbreiten sich entweder über E-Mails oder über Netzwerkpakete. Diesbezüglich werden zwei Arten unterschieden:

- **E-Mail-Würmer –** Würmer, die sich selbstständig über E-Mail-Adressen aus der Kontaktliste eines Nutzers verbreiten.
- **Netzwerkwürmer –** Würmer, die die Sicherheitslücken verschiedener Anwendungen ausnutzen.

Würmer sind daher wesentlich flexibler als Viren. Aufgrund der enormen Ausdehnung des Internets können sich Würmer innerhalb weniger Stunden über den gesamten Globus verbreiten–in manchen Fällen gelingt ihnen dies sogar schon in wenigen Minuten. Wegen dieser Fähigkeit, sich unabhängig und rasant zu vermehren, sind Würmer denn auch gefährlicher als andere Arten von Malware, wie z. B. Viren.

Ein in einem System aktiver Wurm kann eine Reihe von Unannehmlichkeiten verursachen: Er kann Dateien löschen, die Systemleistung beeinträchtigen oder gar Programme deaktivieren. Aufgrund ihrer Beschaffenheit können Würmer als Transportmedium für andere Arten von Angriffen fungieren.

Ist Ihr Computer von einem Wurm infiziert worden, empfiehlt es sich, alle betroffenen Dateien zu löschen, da sie höchstwahrscheinlich Schadcodes enthalten.

Zu den bekanntesten Würmern zählen: Lovsan/Blaster, Stration/Warezov, Bagle und Netsky.

6.1.3 Trojaner

Trojaner galten früher als eine Klasse von Schadprogrammen, die sich als nützliche Anwendungen tarnen, um den Benutzer zur Ausführung zu verleiten. Dies gilt jedoch nur für die Trojaner von damals. Heutzutage müssen sich Trojaner nicht mehr tarnen. Ihr einzige Absicht besteht darin, sich möglichst leicht Zugang zu einem System zu verschaffen, um dort den gewünschten Schaden anzurichten. Der Begriff „Trojaner" ist zu einem sehr allgemeinen Begriff geworden, der jegliche Form von Schadsoftware beschreibt, die nicht einer bestimmten Kategorie zugeordnet werden kann.

Aus diesem Grund wird die Kategorie „Trojaner" oft in mehrere Gruppen unterteilt. Die bekanntesten davon sind:

- Downloader–Ein bösartiges Programm zum Herunterladen von Schadsoftware aus dem Internet.
- Dropper–Trojaner, der auf angegriffenen Computern weitere Malware absetzt („droppt").
- Backdoor–Anwendung, die Angreifern Zugriff auf ein System verschafft, um es zu kontrollieren.
- Keylogger–Programm, das die Tastenanschläge eines Benutzers aufzeichnet und die Informationen an Angreifer sendet.
- Dialer–Dialer sind Programme, die Verbindungen zu teuren Einwahlnummern herstellen. Dass eine neue Verbindung erstellt wurde, ist für den Benutzer nahezu unmöglich festzustellen. Dialer sind nur eine Gefahr für Benutzer von Einwahlmodems. Darum werden Dialer auch nur noch selten eingesetzt.

Trojaner sind in der Regel ausführbare Dateien mit der Erweiterung „.exe". Wenn auf Ihrem Computer eine Datei als Trojaner identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

Zu den bekanntesten Trojanern zählen: NetBus, Trojandownloader. Small.ZL, Slapper

6.1.4 Rootkits

Rootkits sind bösartige Programme, die Hackern unbegrenzten und verdeckten Zugriff auf ein System verschaffen. Nach dem Zugriff auf ein System (in der Regel unter Ausnutzung einer Sicherheitslücke) greifen Rootkits auf Funktionen des Betriebssystems zurück, um nicht von der Virenschutz-Software erkannt zu werden: Prozesse, Dateien und Windows-Registrierungsdaten werden versteckt. Aus diesem Grund ist es nahezu unmöglich, Rootkits mithilfe der üblichen Prüfmethoden zu erkennen.

Bei der Rootkit-Prävention müssen Sie beachten, dass Rootkits auf zwei verschiedenen Ebenen erkannt werden können:

1. Beim Zugriff auf ein System. Die Rootkits haben das System noch nicht befallen, sind also inaktiv. Die meisten Virenschutzsysteme können Rootkits auf dieser Ebene entfernen (vorausgesetzt, dass solche Dateien auch als infizierte Dateien erkannt werden).

2. Wenn sich die Rootkits vor den regulären Prüfmethoden verstecken. Benutzer des ESET-Virenschutzsystems profitieren von dem Vorteil der Anti-Stealth-Technologie, die auch aktive Rootkits erkennen und entfernen kann.

6.1.5 Adware

Adware ist eine Abkürzung für durch Werbung (engl. Advertising) unterstützte Software. In diese Kategorie fallen Programme, die zur Anzeige von Werbung dienen. Adware-Anwendungen öffnen häufig in Internetbrowsern neue Popup-Fenster mit Werbung oder ändern die Startseite des Browsers. Adware gehört oftmals zu Freeware-Programmen, da die Entwickler auf diesem Weg die Entwicklungskosten ihrer (gewöhnlich nützlichen) Anwendungen decken können.

Adware selbst ist nicht gefährlich–allerdings werden die Benutzer mit Werbung belästigt. Bedenklich ist Adware, insofern sie auch dazu dienen kann, Daten zu sammeln (wie es auch bei Spyware der Fall ist).

Wenn Sie sich dafür entscheiden, ein Freeware-Produkt zu verwenden, sollten Sie bei der Installation besonders aufmerksam sein. Die meisten Installationsprogramme benachrichtigen Sie über die Installation eines zusätzlichen Adware-Programms. In vielen Fällen ist es möglich, diesen Teil der Installation abzubrechen und das Programm ohne Adware zu installieren. In einigen Fällen lassen sich Programme jedoch ohne die Adware nicht oder nur mit eingeschränktem Funktionsumfang installieren. Das bedeutet, dass Adware häufig ganz „legal" auf das System zugreift, da sich die Benutzer damit einverstanden erklärt haben. In diesem Fall gilt: Vorsicht ist besser als Nachsicht.

Wenn auf Ihrem Computer eine Datei als Adware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.6 Spyware

Der Begriff „Spyware" fasst alle Anwendungen zusammen, die vertrauliche Informationen ohne das Einverständnis/ Wissen des Benutzers versenden. Diese Programme verwenden Überwachungsfunktionen, um verschiedene statistische Daten zu versenden, z. B. Listen der besuchten Websites, E-Mail-Adressen aus dem Adressbuch des Benutzers oder eine Auflistung von Tastatureingaben.

Die Autoren von Spyware geben vor, auf diesem Weg die Interessen und Bedürfnisse der Benutzer erkunden zu wollen. Ziel sei es, gezieltere Werbeangebote zu entwickeln. Das Problem dabei ist, dass nicht wirklich zwischen nützlichen und bösartigen Anwendungen unterschieden werden kann. Niemand kann sicher sein, dass die gesammelten Informationen nicht missbraucht werden. Die von Spyware gesammelten Daten können Sicherheitscodes, PINs, Kontonummern usw. umfassen. Spyware wird oft im Paket mit der kostenlosen Version eines Programms zum Download angeboten, um Einkünfte zu erzielen oder einen Anreiz für den Erwerb der kommerziellen Version zu schaffen. Oft werden die Benutzer bei der Programminstallation darüber informiert, dass Spyware eingesetzt wird, um sie damit zu einem Upgrade auf die kommerzielle, Spyware-freie Version zu bewegen.

Beispiele für bekannte Freeware-Produkte, die im Paket mit Spyware ausgeliefert werden, sind Client-Anwendungen für P2P-(Peer-to-Peer-) Netzwerke. Programme wie Spyfalcon oder Spy Sheriff gehören zur einer besonderen Kategorie von Spyware: Getarnt als Spyware-Schutz-Programme üben sie selbst Spyware-Funktionen aus.

Wenn auf Ihrem Computer eine Datei als Spyware identifiziert wird, sollte diese gelöscht werden, da sie mit hoher Wahrscheinlichkeit Schadcode enthält.

6.1.7 Potenziell unsichere Anwendungen

Es gibt zahlreiche rechtmäßige Programme, die die Verwaltung miteinander vernetzter Computer vereinfachen sollen. Wenn sie allerdings missbraucht werden, können sie durchaus schädliche Wirkung haben. Darum wurde von ESET diese spezielle Kategorie geschaffen. Unsere Kunden haben nun die Option, zu wählen, ob solche Bedrohungen vom Virenschutzsystem erkannt werden sollen oder nicht.

Zur Kategorie der „potenziell unsicheren Anwendungen" zählen Programme, die zwar erwünscht sind, jedoch potenziell gefährliche Funktionen bereitstellen. Dazu zählen beispielsweise Programme für das Fernsteuern von Computern (Remotedesktopverbindung), Programme zum Entschlüsseln von Passwörtern und Tastaturrekorder (Programme, die aufzeichnen, welche Tasten vom Benutzer gedrückt werden).

Sollten Sie feststellen, dass auf Ihrem Computer eine potenziell unsichere Anwendung vorhanden ist (die Sie nicht selbst installiert haben), wenden Sie sich an Ihren Netzwerkadministrator oder entfernen Sie die Anwendung.

6.1.8 Eventuell unerwünschte Anwendungen

Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, aber auf Leistung und Verhalten Ihres Computers negative Auswirkungen haben können. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Stand vor der Installation). Die gravierendsten Veränderungen sind:

- Neue Fenster werden angezeigt
- Versteckte Prozesse werden gestartet
- Prozessor und Speicher werden stärker belastet als zuvor
- Suchergebnisse ändern sich
- Die Anwendung kommuniziert mit Servern im Internet

6.2 Remote-Angriffe

Es gibt zahlreiche spezielle Techniken, die es Angreifern ermöglichen, fremde Systeme zu beeinträchtigen. Dabei unterscheidet man zwischen mehreren Kategorien.

6.2.1 DoS-Angriffe

DoS- bzw. Denial of Service-Angriffe zielen darauf ab, Computer-Ressourcen für die eigentlichen Nutzer unzugänglich zu machen. Die Kommunikation zwischen betroffenen Benutzern wird behindert und geht nicht mehr ordnungsgemäß vonstatten. In der Regel müssen Sie einen Computer, der einem DoS-Angriff ausgesetzt ist, neu starten. Nur so ist der ordnungsgemäße Betrieb wiederherzustellen.

In den meisten Fällen sind Webserver betroffen. Ziel solcher Angriffe ist es, die Verfügbarkeit der Webserver für einen bestimmten Zeitraum auszusetzen.

6.2.2 DNS Poisoning

Mithilfe von „DNS Poisoning" können Hacker DNS-Server beliebiger Computer über die Echtheit eingeschleuster Daten täuschen. Die nicht authentischen Daten werden für einige Zeit im Cache gespeichert, so dass Angreifer die DNS-Antworten von IP-Adressen umschreiben können. Dies hat zur Folge, dass Benutzer beim Zugriff auf eine Internet-Website nicht den Inhalt der Website, sondern Computerviren oder Würmer herunterladen.

6.2.3 Angriffe mit Würmern

Bei einem Computerwurm handelt es sich um ein Programm, das einen bösartigen Code enthält, der Hostcomputer angreift und sich über Netzwerke verbreitet. Netzwerkwürmer nutzen die Sicherheitslücken verschiedener Anwendungen aus. Aufgrund der Verfügbarkeit des Internets können sie sich innerhalb weniger Stunden nach ihrer Freigabe über den gesamten Globus verbreiten. In manchen Fällen gelingt ihnen dies sogar in Minutenschnelle.

Ein Großteil der Wurmangriffe (Sasser, SqlSlammer) lässt sich durch Anwendung der Standardsicherheitseinstellungen der Firewall oder durch das Blockieren ungeschützter und unbenutzter Ports vermeiden. Darüber hinaus ist es unerlässlich, dass Sie Ihr System regelmäßig mit den neuesten Sicherheitspatches ausstatten.

6.2.4 Portscans (Port Scanning)

Beim Port Scanning wird ein Netzwerkhost auf offene Computerports untersucht. Ein Portscanner ist eine Software zur Erkennung solcher Ports.

Bei einem Computerport handelt es sich um einen virtuellen Punkt zur Abwicklung von ein- und ausgehenden Daten. Für die Sicherheit spielen Ports eine zentrale Rolle. In einem großen Netzwerk können die von Portscannern gesammelten Informationen dazu beitragen, mögliche Sicherheitslücken ausfindig zu machen. Diese Art der Nutzung ist legitim.

Dennoch wird Port Scanning oft von Hackern missbraucht, um Sicherheitsbestimmungen zu unterlaufen. In einem ersten Schritt werden Pakete an jeden Port gesendet. Aus der Art der Rückmeldung lässt sich ableiten, welche Ports verwendet werden. Der Port Scanning-Vorgang selbst verursacht keinen Schaden. Seien Sie sich jedoch im Klaren darüber, dass auf diese Weise Sicherheitslücken aufgedeckt werden können und Angreifer dadurch die Möglichkeit haben, die Kontrolle über Remotecomputer zu übernehmen.

Netzwerkadministratoren wird geraten, alle inaktiven Ports zu blockieren und alle aktiven Ports vor unerlaubtem Zugriff zu schützen.

6.2.5 TCP Desynchronization

Die Technik der TCP Desynchronization wird für TCP-Hijacking-Angriffe eingesetzt. Die TCP Desynchronization wird ausgelöst, wenn die Laufnummer der eingehenden Pakete sich von der erwarteten Laufnummer unterscheidet. Die Pakete mit unerwarteter Laufnummer werden verworfen (oder im Pufferspeicher gespeichert, wenn sie im aktuellen Kommunikationsfenster vorkommen).

Im Zustand der Desynchronisation werden empfangene Pakete von beiden Kommunikationsendpunkten verworfen. Das ist der Zeitpunkt, an dem Angreifer Schadcode und Pakete mit der richtigen Laufnummer einschleusen können. Die Angreifer können die Kommunikation über Befehle oder auf anderem Weg manipulieren.

TCP-Hijacking-Angriffe zielen auf die Unterbrechung von Server-Client- bzw. P2P-Verbindungen. Viele Angriffe können durch Authentifizierungsmaßnahmen für jedes TCP-Segment vermieden werden. Sie sollten Ihre Netzwerkgeräte außerdem gemäß Empfehlung konfigurieren.

6.2.6 SMB Relay

SMBRelay und SMBRelay2 sind besondere Programme zum Ausführen von Angriffen auf Remotecomputern. Die Programme nutzen das SMB-Protokoll, das auf NetBIOS aufbaut, für den gemeinsamen Datenzugriff. Für die Freigabe eines Ordners oder eines Verzeichnisses im LAN wird in der Regel das SMB-Protokoll verwendet.

Im Rahmen der lokalen Netzwerkkommunikation werden Passwort-Hash-Werte ausgetauscht.

SMBRelay empfängt eine Verbindung über die UDP-Ports 139 und 445, leitet die zwischen Client und Server ausgetauschten Pakete weiter und manipuliert sie. Nachdem die Verbindung hergestellt wurde und die Authentifizierung erfolgt ist, wird die Verbindung zum Client getrennt. SMBRelay erstellt eine neue virtuelle IP-Adresse. Auf die neue Adresse kann über den Befehl „net use \\192.168.1.1" zugegriffen werden. Jede der Windows-Netzwerkfunktionen kann dann auf diese Adresse zugreifen. Bis auf Aushandlungs- und Authentifizierungsdaten leitet SMBRelay alle SMB-Protokoll-Daten weiter. Angreifer können die IP-Adresse verwenden, solange der Client-Computer verbunden ist.

SMBRelay2 funktioniert nach demselben Prinzip wie SMBRelay, verwendet aber NetBIOS-Namen statt IP-Adressen. Beide können Man-in-the-Middle-Angriffe ausführen. Über diese Art von Angriffen können Angreifer Nachrichten, die zwischen zwei Kommunikationsendpunkten ausgetauscht werden, unbemerkt lesen und manipulieren. Computer, die solchen Angriffen ausgesetzt sind, senden häufig keine Antwort mehr oder werden ohne ersichtlichen Grund neu gestartet.

Um Angriffe zu vermeiden, sollten Sie Authentifizierungspasswörter oder -schlüssel verwenden.

6.2.7 ICMP-Angriffe

ICMP (Internet Control Message Protocol) ist ein weitverbreitetes Internetprotokoll. Es wird vor allem verwendet, um Fehlermeldungen von vernetzten Computern zu senden.

Angreifer versuchen, die Schwachstellen des ICMP-Protokolls auszunutzen. ICMP wird für einseitige Kommunikation eingesetzt, bei der keine Authentifizierung erforderlich ist. Dadurch können Angreifer sogenannte DoS (Denial of Service)-Angriffe starten oder Angriffe ausführen, durch die nicht autorisierte Personen auf eingehende und ausgehende Datenpakete zugreifen können.

Typische Beispiele für ICMP-Angriffe sind Ping-Flood, ICMP_ ECHO-Flood und Smurf-Attacken. Bei einem ICMP-Angriff arbeitet der Computer deutlich langsamer (dies gilt für alle Internetanwendungen), und es treten Probleme mit der Internetverbindung auf.

6.3 E-Mail

E-Mail („elektronische Post") ist ein modernes Kommunikationsmittel mit vielen Vorteilen. Sie ist flexibel, schnell und direkt. Bei der Verbreitung des Internets in den frühen 1990er Jahren spielte E-Mail eine entscheidende Rolle.

Doch aufgrund der Anonymität, die E-Mails und das Internet bieten, wird diese Kommunikationsform auch häufig für illegale Aktivitäten wie das Versenden von Spam-Mails genutzt. Als „Spam" gelten z. B. unerwünschte Werbeangebote, Hoaxes (Falschmeldungen) und E-Mails, mit denen Schadsoftware verbreitet werden soll. Die Belästigung und Gefährdung durch Spam wird zusätzlich dadurch gefördert, dass E-Mails praktisch kostenlos versendet werden können und den Verfassern von Spam-Mails verschiedenste Tools und Quellen zur Verfügung stehen, um an neue E-Mail-Adressen zu gelangen. Die große Anzahl und Vielfalt, in der Spam-Mails auftreten, erschweren die Kontrolle. Je länger Sie eine E-Mail-Adresse verwenden, desto wahrscheinlicher ist es, dass diese in einer Spam-Datenbank erfasst wird. Einige Tipps zur Vorbeugung:

- Veröffentlichen Sie Ihre E-Mail-Adresse, soweit möglich, nicht im Internet.
- Geben Sie Ihre E-Mail-Adresse nur an vertrauenswürdige Personen weiter.
- Benutzen Sie, wenn möglich, keine üblichen Aliasnamen– bei komplizierten Aliasnamen ist die Wahrscheinlichkeit der Verfolgung niedriger.

- Antworten Sie nicht auf Spam-Mails, die sich in Ihrem Posteingang befinden.
- Seien Sie vorsichtig, wenn Sie Internetformulare ausfüllen–achten Sie insbesondere auf Kontrollkästchen wie „Ja, ich möchte per E-Mail über ... informiert werden".
- Verwenden Sie separate E-Mail-Adressen–z. B. eine für Ihre Arbeit, eine für die Kommunikation mit Freunden usw.
- Ändern Sie Ihre E-Mail-Adresse von Zeit zu Zeit.
- Verwenden Sie eine Spam-Schutz-Lösung.

6.3.1 Werbung

Werbung im Internet ist eine der am schnellsten wachsenden Formen von Werbung. Bei der E-Mail-Werbung werden E-Mail-Nachrichten als Kommunikationsmedium verwendet. Die wesentlichen Vorteile für das Marketing liegen im geringen finanziellen Aufwand, dem hohen Grad von Direktheit und der Effektivität. Davon abgesehen erreichen E-Mails die Empfänger fast ohne Zeitverzögerung. In vielen Unternehmen werden E-Mail-Marketingtools für eine effektive Kommunikation mit aktuellen und zukünftigen Kunden verwendet.

Da Benutzer Interesse an kommerziellen Informationen zu bestimmten Produkten haben können, handelt es sich um rechtmäßige Werbung. Dem gegenüber steht die Tatsache, dass vielfach unerwünschte Massen-E-Mails mit Werbung versendet werden. In solchen Fällen ist die Grenze der E-Mail-Werbung überschritten, und diese E-Mails gelten als Spam.

Die Masse der unerwünschten Werbe-E-Mails hat sich zu einem echten Problem entwickelt, bei dem kein Nachlassen abzusehen ist. Die Verfasser unerwünschter E-Mail versuchen naturgemäß, Spam-E-Mails wie rechtmäßige Nachrichten aussehen zu lassen. Andererseits kann auch rechtmäßige Werbung im Übermaß negative Reaktionen hervorrufen.

6.3.2 Falschmeldungen (Hoaxes)

Ein Hoax ist eine Spam-Nachricht, die über das Internet verbreitet wird. Hoaxes werden per E-Mail oder über Kommunikationstools wie ICQ oder Skype versendet. Der Inhalt der Nachricht ist meist ein Scherz oder eine Falschmeldung.

Oft werden dabei Falschmeldungen zu angeblichen Computerviren verbreitet. Der Empfänger soll verunsichert werden, indem ihm mitgeteilt wird, dass sich auf seinem Computer ein „nicht identifizierbarer Virus" befindet, der Dateien zerstört, Passwörter abruft oder andere schädliche Vorgänge verursacht.

Andere Hoaxes zielen darauf ab, den Empfänger emotional zu belästigen. Der Empfänger wird üblicherweise aufgefordert, die Nachricht an alle seine Kontakte weiterzuleiten, wodurch der Lebenszyklus des Hoax verlängert wird. Es gibt verschiedenste Arten von Hoaxes–Mobiltelefon-Hoaxes, Hilferufe, Angebote zu Geldüberweisungen aus dem Ausland usw. In den meisten Fällen ist es nicht möglich, die tatsächliche Absicht des Autors zu prüfen.

Wenn Sie eine Nachricht lesen, in der Sie dazu aufgefordert werden, diese an alle Ihre Kontakte weiterzuleiten, handelt es sich möglicherweise um einen Hoax. Es gibt spezielle Internetseiten, auf denen Sie prüfen können, ob eine E-Mail rechtmäßig ist oder nicht. Bevor Sie eine fragliche Nachricht weiterleiten, versuchen Sie, über die Internetsuche abzuklären, ob es sich um einen Hoax handelt.

6.3.3 Phishing

Der Begriff „Phishing" bezeichnet eine kriminelle Vorgehensweise, die sich Techniken des Social Engineering (Manipulation von Benutzern zur Erlangung vertraulicher Informationen) zunutze macht. Das Ziel von Phishing ist es, an vertrauliche Daten wie Kontonummern, PIN-Codes usw. zu gelangen.

Der Zugriff auf vertrauliche Informationen wird oft durch das Versenden von E-Mails erlangt, die von einer scheinbar vertrauenswürdigen Person bzw. von einem scheinbar seriösen Unternehmen (Finanzinstitut, Versicherungsunternehmen) stammen. Eine solche E-Mail kann sehr echt aussehen. Grafiken und Inhalte wurden möglicherweise sogar von der Quelle entwendet, die nachgeahmt werden soll. Sie werden unter einem Vorwand (Datenprüfung, finanzielle Transaktionen etc.) aufgefordert, persönliche Daten einzugeben, zum Beispiel Ihre Bankverbindung, Benutzernamen und Passwörter. Alle diese Daten, werden Sie denn übermittelt, können mühelos gestohlen oder missbraucht werden.

Es soll an dieser Stelle darauf hingewiesen werden, dass Banken, Versicherungen und andere rechtmäßige Unternehmen nie in einer E-Mail nach Benutzernamen und Passwort fragen.

6.3.4 Erkennen von Spam-Mails

Es gibt verschiedene Anzeichen, die darauf hindeuten, dass es sich bei einer fraglichen E-Mail in Ihrem Postfach um Spam handelt. Wenn eines oder mehrere der folgenden Kriterien zutreffen, handelt es sich höchstwahrscheinlich um eine Spam-Nachricht:

- Die Adresse des Absenders steht nicht in Ihrer Kontaktliste.
- Ihnen wird ein größerer Geldbetrag in Aussicht gestellt, Sie sollen jedoch zunächst eine kleinere Summe zahlen.
- Sie werden unter einem Vorwand (Datenprüfung, finanzielle Transaktionen etc.) aufgefordert, persönliche Daten einzugeben, wie Ihre Bankverbindung, Benutzernamen und Passwörter.
- Die Nachricht ist in einer anderen Sprache verfasst.
- Sie werden aufgefordert, ein Produkt zu erwerben, das Sie nicht bestellt haben. Falls Sie das Produkt dennoch kaufen möchten, prüfen Sie, ob der Absender ein vertrauenswürdiger Anbieter ist (fragen Sie beim Hersteller nach).
- Einige Wörter sind falsch geschrieben, um den Spamfilter zu umgehen (beispielsweise „vaigra" statt „viagra").

6.3.4.1 Regeln

Bei Spam-Schutz-Lösungen und E-Mail-Programmen dienen Regeln der Steuerung von E-Mail-Funktionen. Regeln setzen sich aus zwei logischen Teilen zusammen:

1. einer Bedingung (z. B. einer eingehenden Nachricht von einer bestimmten Adresse)
2. einer Aktion (z. B. dem Löschen der Nachricht oder dem Verschieben der Nachricht in einen bestimmten Ordner).

Je nach Spam-Schutz-Lösung gibt es unterschiedlich viele Regeln und Kombinationsmöglichkeiten. Regeln dienen als Maßnahme gegen Spam (unerwünschte E-Mail-Nachrichten). Typische Beispiele sind:

- 1. Bedingung: Eine eingehende E-Mail-Nachricht enthält einige der Wörter, die häufig in Spam-Nachrichten vorkommen
  2. Aktion: Nachricht löschen
- 1. Bedingung: Eine eingehende E-Mail-Nachricht enthält einen Anhang mit der Erweiterung EXE
  2. Aktion: Anhang löschen und Nachricht dem Postfach zustellen
- 1. Bedingung: Der Absender einer eingehenden Nachricht ist Ihr Arbeitgeber
  2. Aktion: Nachricht in den Ordner „Geschäftlich" verschieben

Wir empfehlen Ihnen, in Spam-Schutz-Programmen verschiedene Regeln miteinander zu kombinieren, um die Verwaltung zu vereinfachen und den Spam-Schutz noch effektiver zu gestalten.

6.3.4.2 Bayesscher Filter

Die bayessche Filtermethode ist eine sehr effektive Form der E-Mail-Filterung, die in fast allen Spam-Schutz-Produkten verwendet wird. Damit lassen sich unerwünschte E-Mails mit hohem Genauigkeitsgrad erkennen. Der bayessche Filter kann für einzelne Benutzer angewendet werden.

Bayessche Filter funktionieren nach folgendem Prinzip: In der ersten Phase findet ein Lernprozess statt. Der Benutzer kennzeichnet manuell eine ausreichende Anzahl von E-Mails als rechtmäßig oder als Spam (gewöhnlich 200/200). Der Filter analysiert beide Kategorien und lernt beispielsweise, dass in Spam-E-Mails häufig die Wörter „Rolex" oder „Viagra" auftreten oder dass legitime E-Mails von Familienmitgliedern oder von Adressen in der Kontaktliste des Benutzers abgesendet werden. Nach der Bearbeitung einer größeren Zahl von E-Mails kann der bayessche Filter jede Nachricht einem Spam-Index zuordnen und somit entscheiden, ob die Nachricht Spam ist oder nicht.

Der größte Vorteil dieses Filters liegt in seiner Flexibilität. Ist ein Benutzer etwa Biologe, erhalten alle eingehenden E-Mails in Bezug auf Biologie oder ein verwandtes Forschungsfeld im Allgemeinen einen geringen Wahrscheinlichkeitsindex. Wenn eine E-Mail Wörter enthält, durch die sie eigentlich als unerwünscht klassifiziert würde, der Absender jedoch zu den Kontakten des Benutzers gehört, wird die E-Mail als rechtmäßig eingestuft, da sich bei Absendern aus der eigenen Kontaktliste die Gesamtwahrscheinlichkeit für Spam verringert.

6.3.4.3 Whitelist

Im Allgemeinen handelt es sich bei einer Whitelist um eine Liste von Objekten oder Personen, die akzeptiert werden oder denen eine Zugriffsberechtigung eingeräumt worden ist. Der Begriff „E-Mail-Whitelist" bezeichnet eine Liste von Kontakten, von denen der Nutzer Nachrichten erhalten möchte. Solche Whitelists beruhen auf Stichwörtern, nach denen E-Mail-Adressen, Domain-Namen oder IP-Adressen durchsucht werden.

Ist bei einer Whitelist der „Exklusiv-Modus" aktiviert, werden Nachrichten von jeder anderen Adresse, Domain oder IP-Adresse zurückgewiesen. Ist dieser Modus jedoch nicht aktiviert, werden solche Nachrichten nicht etwa gelöscht, sondern auf andere Art und Weise geprüft.

Eine Whitelist beruht somit auf einem Prinzip, das dem einer Blacklist entgegengesetzt ist. Im Vergleich zu Blacklists sind Whitelists relativ pflegeleicht. Es wird empfohlen, sowohl eine Whitelist als auch eine Blacklist zu verwenden, damit Spam effektiver gefiltert werden kann.

6.3.4.4 Blacklist

Eine Blacklist bezeichnet im Allgemeinen eine Liste unerwünschter oder verbotener Personen oder Objekte. In der virtuellen Welt handelt es sich um eine Technik, die das Annehmen von E-Mail-Nachrichten aller Absender erlaubt, die nicht in einer solchen Liste stehen.

Es gibt zwei Arten von Blacklists. Benutzer können über ihr Spam-Schutz-Programm individuelle Blacklists erstellen. Zum anderen sind viele professionelle, von spezialisierten Institutionen erstellte und regelmäßig aktualisierte Blacklists im Internet verfügbar.

Eine Blacklist basiert auf einem Prinzip, das dem einer Whitelist entgegengesetzt ist. Das Verwenden von Blacklists ist eine wesentliche Technik zur erfolgreichen Spam-Filterung. Allerdings sind Blacklists sehr schwierig zu pflegen, da täglich neue Einträge anfallen. Es wird empfohlen, sowohl eine Whitelist als auch eine Blacklist zu verwenden, damit Spam effektiver gefiltert werden kann.

6.3.4.5 Serverseitige Kontrolle

Die serverseitige Kontrolle ist eine Technik zur Erkennung von massenweise versendeten Spam-E-Mails auf Basis der Anzahl empfangener Nachrichten und der Reaktionen von Benutzern. Jede E-Mail-Nachricht hinterlässt einen eindeutigen digitalen Footprint („Fußabdruck") auf dem Server, der sich nach dem Inhalt der Nachricht richtet. Tatsächlich handelt es sich um eine eindeutige ID-Nummer, die keine Rückschlüsse über den Inhalt der E-Mail zulässt. Zwei identische Nachrichten besitzen denselben Footprint, verschiedene E-Mails auch verschiedene Footprints.

Wenn eine E-Mail als Spam eingestuft wird, wird der Footprint dieser E-Mail an den Server gesendet. Wenn der Server weitere identische Footprints empfängt (die einer bestimmten Spam-E-Mail entsprechen), wird dieser Footprint in einer Datenbank gespeichert. Beim Prüfen eingehender E-Mails sendet das Programm die Footprints der E-Mails an den Server. Der Server gibt Informationen darüber zurück, welche Footprints E-Mails entsprechen, die von Benutzern bereits als Spam eingestuft worden sind.